Capítulo 1

# *INTRODUCCION A LAS REDES*

## 1.1. Concepto de red

La importancia que hoy en día tiene la información es indiscutible, ésta información es manipulada, tratada y formateada, utilizando computadoras interconectadas entre si formando una *red*.

Red de computadoras, es una colección interconectada de computadoras autónomas. Dos computadoras se consideran interconectadas cuando son capaces de intercambiar información

Una ***red*** en general es un sistema de transmisión de datos que permite el intercambio de información entre dispositivos electrónicos (computadores) que toman el nombre de ***HOST***. El ***HOST*** es todo dispositivo electrónico (computador) conectado a una red.

En definición más específica, una ***red*** es un conjunto de computadoras que van a compartir archivos (carpetas, datos, imágenes, audio, video, etc.) o recursos (disco duro, lectora, disketera, monitor, impresora, fotocopiadora, web cam, etc.), éstas computadoras pueden estar interconectadas por un medio físico o inalámbrico.

La transmisión de datos se produce a través de un medio de transmisión o combinación de distintos medios: cables de par trenzado, cables coaxiales, cables de fibra óptica, tecnología inalámbrica, enlace bluetooth, enlace infrarrojo, enlace vía satélite.

Los ***dispositivos electrónicos*** de acceso a redes son por ejemplo: computador personal, impresor, fotocopiador, escáner, cámara de video, asistente personal (PDA), celular, semáforo inteligente centralizado, televisión (Web TV), video vigilancia, refrigerador capaz de intercambiar información (lista de compra) con un supermercado virtual, etc.

Los ***componentes*** principales de una red son:

a. Los nodos de red (estación, servidor, dispositivo de comunicación).
b. Los medios de comunicación (físico, inalámbrico).
c. Los protocolos (TCP, IP, UDP, etc.).

## 1.2. El antes y después de las redes

- ANTES
  - redes especializadas por servicio.
  - velocidades limitadas.
  - conexiones por tiempo limitado.
  - cero movilidad.
- HOY
  - Tráfico de datos superando la voz.
  - Variedad de aplicaciones y servicios separados: internet, video, Datos, etc.
  - Aumento de necesidades por parte del cliente.
  - Limitada movilidad.
- DESPUES
  - Convergencia al lado del cliente: voz, video y datos (triple play).
  - Gran ancho de banda.
  - Servicios en tiempo real.
  - Mi propio internet.
  - Movilidad.

| Antes | Después |
|---|---|
| **Conectividad** | SVA |
| **Narrowband** | Broadband |
| **Conexiones Estáticas** | Conexiones Dinámicas |

- Narrowband: banda estrecha
- Broadband: banda ancha

## 1.3. Banda ancha

"Banda Ancha" es un conjunto de tecnologías que permiten ofrecer a los usuarios altas velocidades de comunicación y conexiones permanentes.

Permite que los proveedores de Servicio ofrezcan una variedad servicios de valor agregado.

Se ofrece a través de una serie de tecnologías y el equipamiento adecuado para llegar al usuario final con servicios de voz, video y datos.

## 1.4. La última milla

¿Qué es la última milla? la última milla es la conexión entre el usuario final y la estación local/ central/hub.

Puede ser alámbrica o Inalámbrica.

Hay tres problemas con la última milla:

- La infraestructura de última milla tiene el costo más alto de todos los elementos de una red. Los costos iniciales son altos, especialmente si se hace necesaria ductería.
- Hay pocos usuarios en áreas rurales, y eso significa que la “milla intermedia” (desde el punto de acceso a la red de core) no se comparte eficientemente.
- Por lo tanto se ofrecen altos precios a los clientes.

## 1.5. Selección de tecnologías

La selección de la tecnología condiciona los servicios que se pueden ofrecer:

- condiciona el ancho de banda.
- condiciona el monto de inversión.
- condiciona los costos de operación y de venta.

La selección de la tecnología debe estar sólidamente basada en el modelo del negocio:

- La tecnología seleccionada debe ser actual y estar disponible.
- Siempre se deben estudiar los modelos de negocio exitosos en otros países y juzgar hasta qué punto el negocio es viable.

## 1.6. Tecnologías de acceso

Tecnologías Alámbricas:

- Redes de Acceso por par de Cobre (xDSL, Modems)
- Redes de Acceso por Cable.
- Redes híbridas de fibra y cable (HFC).
- Acceso Fijo por Red eléctrica (PLC).
- Redes de Acceso por Fibra óptica (FTTx, PON, EFM, otros).

Tecnologías Inalámbricas:

- Bucle inalámbrico (WiLL o Wireless Local Loop, LMDS, MMDS).
- Redes MAN/LAN inalámbricas (WLAN, Wi-Fi, WiMAX, HiperLAN2).
- Comunicaciones móviles de segunda y tercera generación (CDMA, GSM, UMTS, 3G).
- Óptica por Aire (HAPs, FSO).
- Redes de acceso por satélite.
- Televisión digital terrestre (TDT).

## 1.7. Tecnologías de transporte

¿Qué pasa por detrás de la última milla? Las señales viajan por redes de transporte, a través de diferentes tecnologías:

CAPA 1

- Redes SDH.
- Redes ópticas transparentes (OTH).
- Cobre, Microondas y otros medios ...

CAPA 2

- Redes ATM.
- Redes Frame Relay.
- Redes basadas en Ethernet.

CAPA 3

- Redes Basadas en IP, IP/MPLS.

## 1.8. Clasificación de red

Existen diversos tipos de redes para ser utilizados, que se clasifican por las siguientes características:

a. Por alcance, tamaño o escala (WPAN, LAN, MAN, WAN).
b. Por procesamiento (centralizada, distribuida).
c. Por dependencia del servidor (autónomo, cliente-servidor).
d. Según la tecnología de transmisión usada.

Dado la revolución de las comunicaciones entre computadoras a partir de los años 70, se han producido varios hechos trascendentales, siendo el más importante la conclusión que no existe diferencia fundamental entre procesamiento de datos (computadoras) y comunicación de datos

(equipos de conmutación y transmisión). Consecuentemente se desarrollan sistemas integrados que transmiten y procesan todo tipo de datos e información, donde la tecnología y las organizaciones de normatividad técnica (ISO/OSI, EIA/TIA, IEEE) están dirigiéndose hacia un único sistema público que integre todas las comunicaciones y de uniforme acceso mundial.

### 1.2.1. Clasificación según su alcance, tamaño o escala:

***Red WPAN*** (*Wireless Personal Area Networks*, red inalámbrica de área personal) es una red de computadoras para la comunicación entre distintos dispositivos (tanto computadoras, puntos de acceso a internet, teléfonos celulares, PDA, dispositivos de audio, impresoras) cercanos al punto de acceso. Estas redes normalmente son de unos pocos metros y para uso personal, así como fuera de ella.

***Red LAN*** (*Local Area Network*, red de área local) son las redes de un centro de cómputo, oficina, edificio. Debido a sus limitadas dimensiones, son redes muy rápidas en las cuales cada dispositivo electrónico (computador) se puede comunicar con el resto.

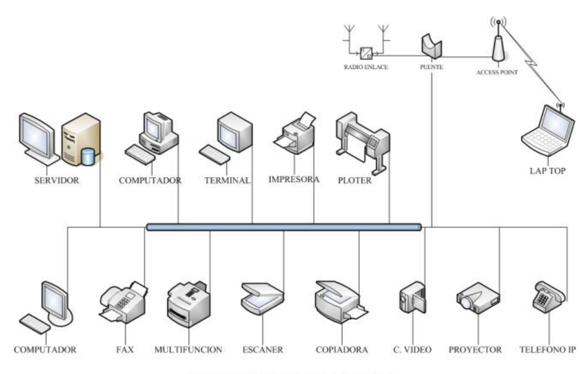



**Ilustración 1**

Una variante de red LAN, es conocida como ***red LAN Múltiple***, que permite interconectar redes LAN vía inalámbrica o alámbrica edificios ubicados dentro de una ciudad o localidades

cercanas (ejemplo: red LAN Múltiple de la UNASAM en la ciudad de Huaraz).

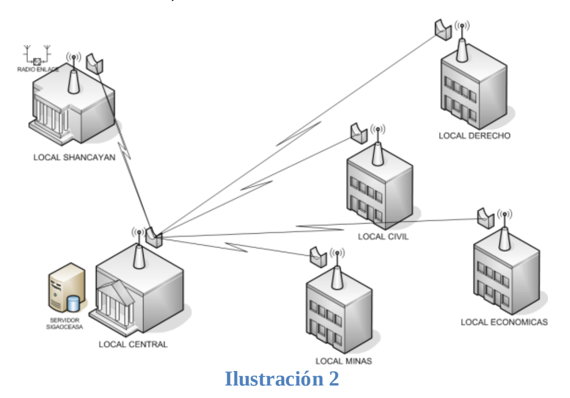



Ilustración 2

***Red MAN*** (*Metropolitan Area Network*, red de área metropolitana) conecta diversas LAN cercanas geográficamente (en un área de alrededor de cincuenta kilómetros) entre sí a alta velocidad. Por lo tanto, una MAN permite que dos nodos remotos se comuniquen como si fueran parte de la misma red de área local. Una MAN está compuesta por conmutadores o routers conectados entre sí con conexiones de alta velocidad (generalmente cables de fibra óptica).

Las redes inalámbricas de área metropolitana (WMAN) también se conocen como bucle local inalámbrico (WLL, Wireless Local Loop). Las WMAN se basan en el estándar IEEE 802.16. Los bucles locales inalámbricos ofrecen una velocidad total efectiva de 1 a 10 Mbps, con un alcance de 4 a 10 kilómetros, algo muy útil para compañías de telecomunicaciones.

La mejor red inalámbrica de área metropolitana es WiMax, que puede alcanzar una velocidad aproximada de 70 Mbps en un radio de varios kilómetros.

***Red WAN*** (*Wide Area Network*, red de área extensa) son redes punto a punto que interconectan ciudades, países y continentes. Al tener que recorrer gran distancia sus velocidades son menores que las redes LAN, aunque son capaces de transportar una mayor cantidad de datos. Por ejemplo, una red troncal de fibra

óptica para interconectar ciudades de un país (red de fibra óptica entre Tumbes y Tacna), un enlace satelital entre países (Perú y EEUU), un cable submarino entre continentes (América y Europa).

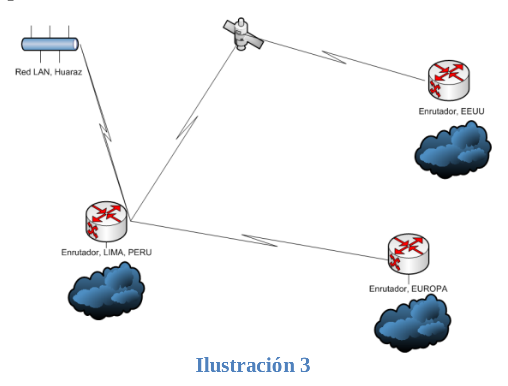
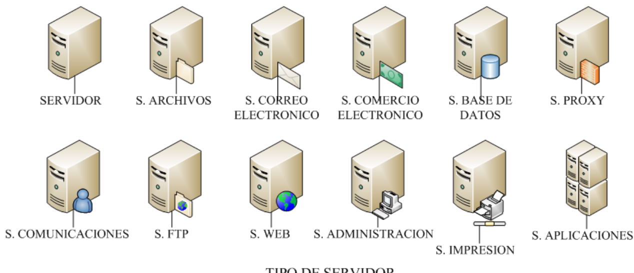



Ilustración 3

### 1.2.2. Clasificación según el procesamiento, dependencia del servidor o distribución lógica

Todo dispositivo electrónico (computador) tiene un lado servidor y otro cliente, puede ser servidor de un determinado servicio pero cliente de otro servicio.

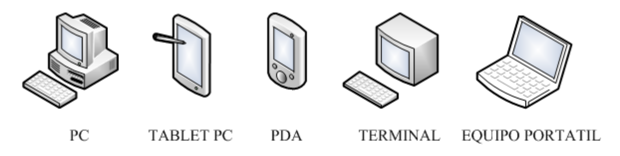
- ***Servidor***. computador que ofrece información o servicios al resto de los dispositivos electrónicos (computador) de la red. La clase de información o servicios que ofrece, determina el tipo de servidor como por ejemplo: servidor de archivos, correo electrónico, comercio electrónico, base de datos, proxy, comunicaciones, FTP, web, administración, impresión, aplicaciones, etc.




TIPO DE SERVIDOR

**Ilustración 4**

- ***Cliente***. Dispositivo electrónico (computador) que accede a la información de los servidores o utiliza sus servicios. Ejemplo: Cada vez que estamos viendo una página web (almacenada en un servidor remoto) nos estamos comportando como clientes. También seremos clientes si utilizamos el servicio de impresión de una impresora conectada a la red.




TIPO DE CLIENTE

**Ilustración 5**

Dependiendo de si existe una función predominante o no para cada nodo de la red, las redes se clasifican en:

- ***Red servidor / cliente.*** Uno o más computadoras actúan como servidores y el resto como clientes. Son las más potentes de la red. No se utilizan como puestos de trabajo. Se pueden administrar de forma remota (Internet es una red basada en la arquitectura cliente/servidor).

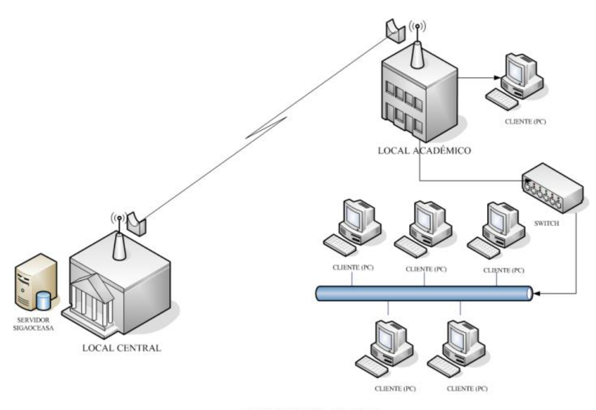



**Ilustración 6**

- ***Redes entre iguales ó autónomo.*** No existe una jerarquía en la red, todas las computadoras pueden actuar como clientes (accediendo a los recursos) o como servidores (ofreciendo recursos).

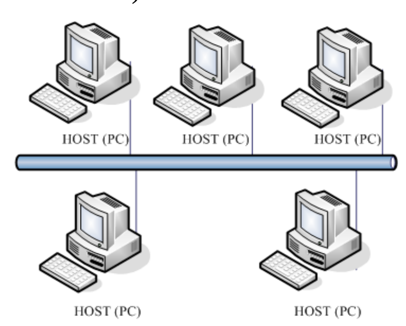



**Ilustración 7**

## *Preguntas propuestas*

1.- ¿Qué es una red de computadores?

2.- ¿Para qué se usan las redes?

3.- ¿Podemos clasificar las redes en las dimensiones de la tecnología de transmisión y del tamaño?

4.- ¿Cuáles son las características de la LAN?

5.- ¿Cuáles son las características de la WAN?

6.- ¿Qué es el Internet?

7.- ¿Qué son las redes inalámbricas?

## *Respuestas a las preguntas propuestas*

1.-

- Un grupo interconectado de dispositivos electrónicos (computadores).

2.-

- *Compartir recursos*, especialmente la información (los datos)
- *Proveer la confiabilidad*, más de una fuente para los recursos
- *La escalabilidad de los recursos computacionales*, si se necesita más poder computacional, se puede comprar un cliente más, en lugar de un nuevo mainframe
- *Comunicación,* correo electrónico, chat, perifoneo.

3.-

- *Tecnología de transmisión*
  - ✓ Broadcast. Un solo canal de comunicación compartido por todas las computadoras. Un paquete mandado por alguna computadora es recibido por todas las otras.
  - ✓ Point-to-point. Muchas conexiones entre pares individuales de computadoras. Los paquetes de A y B pueden atravesar computadoras intermedias, entonces se necesita el ruteo (routing) para dirigirlos.
- *Tamaño (escala)*
  - ✓ LAN (local area network): 10 m a 45 km
  - ✓ WAN (wide area network): 100 km a 1.000 km
  - ✓ Internet: mayor a 10.000 km

4.-

- Normalmente usan la tecnología de broadcast, un solo cable con todas las computadoras conectadas.
- El tamaño es restringido, así el tiempo de transmisión del peor caso es conocido.
- Las velocidades típicas son de 10, 100, 1000 Mbps

5.-

- Consisten en una colección de hosts (computador) o LAN de hosts conectados por una subred.

- La subred consiste en las líneas de transmisión y los ruteadores que son dispositivos electrónicos dedicados a cambiar de ruta.
- Se mandan los paquetes de un ruteador a otro.
- Se dice que la red es packet-switched (paquetes ruteados) o store-and-forward (guardar y reenviar).

6.-

- El internet es una red de redes vinculadas por gateways, que son dispositivos electrónicos que pueden traducir entre formatos incompatibles.

7.-

- Una red inalámbrica usa radio, microondas, satélites, infrarrojo, u otros mecanismos para comunicarse.
- Se pueden combinar las redes inalámbricas con los computadores móviles, pero los dos conceptos son distintos, ejemplos:

**Tabla 1**

| Inalámbrico | Móvil | Aplicación |
|---|---|---|
| **No** | No | Workstations estacionarias |
| **No** | Sí | Uso de una PC portable en un hotel |
| **Sí** | No | LAN en un edificio sin cables |
| **Sí** | Sí | PDA (personal digital assistant) para inventario |

Capítulo 2

# *SISTEMA DE COMUNICACIÓN DE DATOS*

## 2.1. Comunicación de datos

El propósito fundamental de las comunicaciones de datos es el de intercambiar información entre dos sistemas (fuente y destino).

La figura1, muestra un modelo sistémico de comunicaciones, donde:

- La información es introducida mediante un dispositivo de entrada a un Sistema Fuente y que mediante un transmisor es convertida en una señal que depende de las características del medio de transmisión.
- En el otro extremo en el Sistema Destino, el receptor recibe la señal transmitida y es aproximadamente igual a la señal de entrada (información).
- Finalmente, el dispositivo de salida entrega el mensaje (información transmitida)




SISTEMA GENERAL DE COMUNICACIÓN DE DATOS

**Ilustración 8**

## 2.2. Tareas de un sistema de comunicación de datos

Como otro enfoque adicional se muestra a continuación en la Tabla2, las tareas claves que desarrolla un sistema de comunicación de datos, siendo las tareas arbitrarias, pueden ser mezclados, agregados o pueden ser realizados en diferentes niveles del sistema.

**Tabla 2**

| | *Tareas* |
|---|---|
| 1 | Utilización del sistema transmisión |
| 2 | Interface |
| 3 | Generación de señales |
| 4 | Sincronización |
| 5 | Administración de intercambios |
| 6 | Detección y corrección de errores |
| 7 | Control de flujo |
| 8 | Direccionamiento y enrutamiento |
| 9 | Recuperación |
| 10 | Formato del mensaje |
| 11 | Protección |
| 12 | Administración del sistema |

### *Utilización del sistema transmisión*

Necesidad de hacer un uso eficiente de las facilidades de transmisión que son típicamente compartidas entre varios dispositivos de comunicación. Se usan varias técnicas como:

**Tabla 3**

| Técnicas | Característica |
|---|---|
| **Multiplexaje** | Para asignar la capacidad total del medio de transmisión entre varios usuarios. |
| **Control de congestión** | Para que el sistema no se sobrecargue por excesiva demanda de los servicios de transmisión. |

### *Interface*

Para comunicarse, un dispositivo debe tener una Interface con el sistema de transmisión. Mediante el uso de señales electromagnéticas que se propagan sobre un medio de transmisión.

### *Generación de señales*

Se requiere la generación de señales para la comunicación. La propiedad de estas señales, tanto en forma como en intensidad, debe ser capaz de propagarse a través del medio de transmisión y de ser interpretables como datos en el receptor

### *Sincronización*

Tiene que haber alguna forma de sincronización entre el transmisor y receptor. El receptor debe ser capaz de determinar cuando una señal empieza a llegar y cuando termina, así como la duración de cada elemento de señal.

### *Administración de intercambios*

Si los datos deben ser intercambiados en ambas direcciones por un periodo de tiempo, las dos partes deben cooperar. Teniendo en cuenta las convenciones tales como:

- Si ambos dispositivos podrían transmitir simultáneamente o deben hacerlo por turnos.
- La cantidad de datos que debe ser enviado cada vez.
- El formato de los datos.
- Que hacer si se presentan ciertas contingencias como errores.

### *Detección y corrección de errores*

Para circunstancias donde los errores no pueden ser tolerados, se requiere detección y corrección de errores, como el caso de los sistemas de procesamiento de datos.

### *Control de flujo*

Se requiere un control de flujo para que la fuente no sobrecargue el medio ni el destino al enviar datos más rápido de lo que estos puedan ser procesados y absorbidos.

### *Direccionamiento y enrutamiento*

Cuando más de dos dispositivos comparten un medio de transmisión el sistema debe ser informado por la fuente de la identidad de la estación destinataria. El sistema debe asegurar que la estación de destino y sola esa estación, reciba los datos.

### *Recuperación*

Un concepto distinto al de corrección de errores es el recuperación. Esta técnica es necesaria cuando un intercambio de información, tal como una transacción con una base de datos, es interrumpido por una falla en alguna parte del sistema. El objetivo de esta técnica es que el sistema pueda reasumir la actividad en el punto de la interrupción o al

menos que restaure el estado de los sistemas involucrados, a la condición previa al inicio del intercambio de información.

***Formato del mensaje***

Involucra un acuerdo entre ambas partes, la forma de los datos que van intercambiarse. Ambas partes deben usar el mismo código binario de caracteres.

***Protección***

Es importante proporcionar algún grado de protección al sistema de comunicación de datos. El remitente de los datos desearía tener la seguridad de que solo el destinatario recibirá sus datos y viceversa,

***Administración del sistema***

Un sistema de comunicación de datos es tan complejo que no puede funcionar por si mismo. Requiere capacidades de administración del sistema para configurarlo, supervisar su estado, reaccionar ante fallas, sobrecargas y planear inteligentemente su crecimiento futuro

## 2.2. *Conmutación de circuitos, de mensajes y de paquetes*

***Conmutar***, es el procesamiento que realiza un nodo que recibe información de una línea por una determinada interfaz y la reenvía por otra interfaz, con el objetivo de que llegue a un destinatario final (direccionamiento).

La comunicación entre un origen y un destino habitualmente pasa por nodos intermedios que se encargan de encauzar el tráfico. Por ejemplo, en las llamadas telefónicas los nodos intermedios son las centralitas telefónicas y en las conexiones a Internet, los *routers* o encaminadores. Dependiendo de la utilización de estos nodos intermedios, se distingue entre conmutación de circuitos, de mensajes y de paquetes.

- En la ***conmutación de circuitos*** se establece un camino físico entre el origen y el destino durante el tiempo que dure la transmisión de datos. Este camino es exclusivo para los dos extremos de la comunicación: no se comparte con otros usuarios (ancho de banda fijo). Si no se transmiten datos o se transmiten pocos se estará infrautilizando el canal. Las comunicaciones a través de líneas telefónicas analógicas (RTB)

o digitales (RDSI) funcionan mediante conmutación de circuitos.

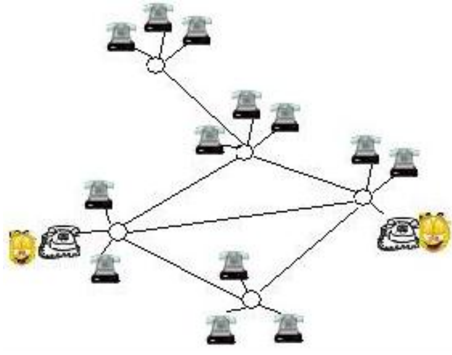


Ilustración 9

- Un mensaje que se transmite por ***conmutación de mensajes*** va pasando desde un nodo al siguiente, liberando el tramo anterior en cada paso para que otros puedan utilizarlo y esperando a que el siguiente tramo esté libre para transmitirlo. Esto implica que el camino origen-destino es utilizado de forma simultánea por distintos mensajes. Sin embargo, éste método no es muy útil en la práctica ya que los nodos intermedios necesitarían una elevada memoria temporal para almacenar los mensajes completos. En la vida real podemos compararlo con el correo postal.




Ilustración 10

- Finalmente, la ***conmutación de paquetes*** es la que realmente se utiliza cuando hablamos de *redes*. Los mensajes se fragmentan en paquetes y cada uno de ellos se envía de forma independiente desde el origen al destino. De esta manera, los nodos (*routers*) no necesitan una gran memoria temporal y el tráfico por la red es más fluido. Nos encontramos aquí con una

serie de problemas añadidos: la pérdida de un paquete provocará que se descarte el mensaje completo; además, como los paquetes pueden seguir rutas distintas puede darse el caso de que lleguen desordenados al destino. Esta es la forma de transmisión que se utiliza en Internet: los fragmentos de un mensaje van pasando a través de distintas redes hasta llegar al destino.

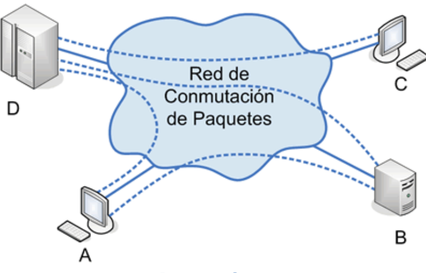



Ilustración 11

## 2.3. Comunicación ***simplex***, ***half-duplex y full-duplex***

- En una comunicación ***simplex*** existe un solo canal unidireccional, el origen puede transmitir al destino pero el destino no puede comunicarse con el origen. Por ejemplo, la radio y la televisión.

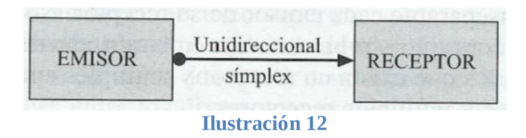



Ilustración 12

- En una comunicación ***half-duplex*** existe un solo canal que puede transmitir en los dos sentidos pero no simultáneamente, las estaciones se tienen que turnar. Esto es lo que ocurre con las emisoras de radioaficionados.

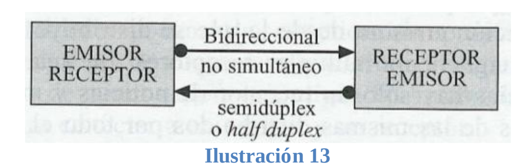



Ilustración 13

- Por último, en una comunicación ***full-duplex*** existen dos canales, uno para cada sentido, ambas estaciones pueden transmitir y recibir a la vez. Por ejemplo, el teléfono.

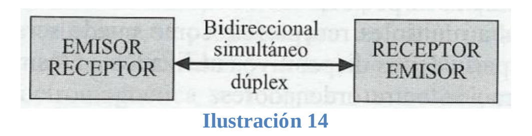



**Ilustración 14**

## 2.4. Mecanismos de ***detección de errores***

¿Cómo puede saber el receptor que ha recibido el mismo mensaje que envió el emisor? ¿Cómo puede saber que no se ha producido ningún error que haya alterado los datos durante la transmisión?

Se necesitan mecanismos de detección de errores para garantizar transmisiones libres de errores. Si el receptor detecta algún error, puede actuar de diversas maneras según los protocolos que esté utilizando. La solución más sencilla es enviarle un mensaje al emisor pidiéndole que le reenvíe de nuevo la información que llegó defectuosa.

Los mecanismos de detección se basan en añadir a las transmisiones una serie de *bits* adicionales, denominados *bits de redundancia*. La redundancia es aquella parte del mensaje que sería innecesaria en ausencia de errores (es decir, no aporta información nueva, sólo permite detectar errores). Algunos métodos incorporan una redundancia capaz de corregir errores. Estos son los *mecanismos de detección y corrección de errores*.

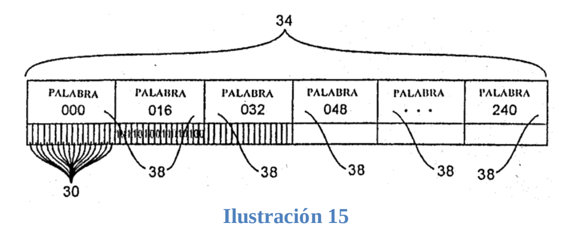



**Ilustración 15**

### *Paridad*

Las transmisiones se dividen en palabras de cierto número de bits (por ejemplo, 8 bits) y se envían secuencialmente. A cada una de estas palabras se le añade un único bit de redundancia (*bit de paridad*) de tal

forma que la suma de todos los bits de la palabra sea siempre un número par (*paridad par*) o impar (*paridad impar*).

El emisor envía las palabras añadiendo los correspondientes bits de paridad. El receptor comprobará a su llegada que la suma de los bits de la palabra incluyendo la redundancia es un número par (si la codificación convenida entre emisor-receptor es de paridad par) o un número impar (paridad impar). Si el receptor encuentra alguna palabra que no se ajuste a la codificación establecida, le solicitará al emisor que le reenvíe de nuevo la información.

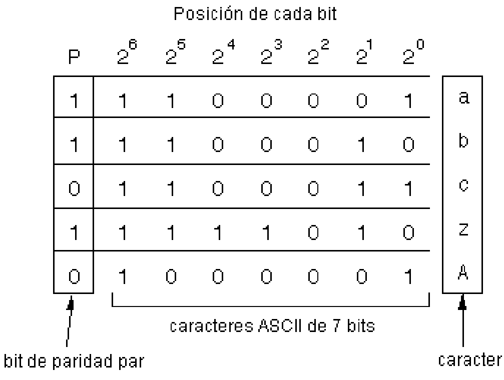



**Ilustración 16**

La paridad únicamente permite detectar errores simples, esto es, que varíe un único bit en cada palabra. Si varían 2 bits, este mecanismo no es capaz de detectar el error.

Veamos un ejemplo de paridad par:

**Tabla 4**

| **Datos** ***(8 bits)*** | **Datos + redundacia** ***(9 bits)*** | **Suma de bits** |
|---|---|---|
| **10110110** | 10110110**1** | 6 |
| **00101001** | 00101001**1** | 4 |
| **11001001** | 11001001**0** | 4 |
| **11111010** | 11111010**0** | 6 |
| **00010000** | 00010000**1** | 2 |

El receptor realizará la suma de bits a la llegada del mensaje. Si alguna palabra no suma un número par, significará que se ha producido un error durante la transmisión.

### *CRC (Código de Redundancia Cíclica)*

Los códigos de paridad tienen el inconveniente de que se requiere demasiada redundancia para detectar únicamente errores simples. En el ejemplo que hemos visto, sólo 8 de 9 bits de información transmitida contenían datos, el resto era redundancia.

Los ***códigos de redundancia cíclica (CRC)*** son muy utilizados en la práctica para la detección de errores en largas secuencias de datos. Se basan en representar las cadenas de datos como polinomios. El emisor realiza ciertas operaciones matemáticas antes de enviar los datos. El receptor realizará, a la llegada de la transmisión, una división entre un polinomio convenido (*polinomio generador*). Si el resto es cero, la transmisión ha sido correcta. Si el resto es distinto significará que se han producido errores y solicitará la retransmisión al emisor.

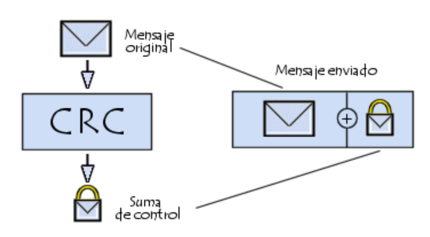



**Ilustración 17**

## *2.5. Control de flujo*

El control de flujo determina cómo enviar la información entre el emisor y el receptor de forma que se vaya recibiendo correctamente sin saturar al receptor. Nótese que puede darse el caso de un emisor rápido y un receptor lento (o un receptor rápido pero que esté realizando otras muchas tareas).

El mecanismo más sencillo de control de flujo se basa en devolver una *confirmación* o *acuse de recibo* (ACK) cada vez que el receptor reciba algún dato correcto o una señal de error (NACK) si el dato ha llegado

dañado. Cuando el emisor recibe un ACK pasa a enviar el siguiente dato. Si, en cambio, recibe un NACK reenviará el mismo dato.

El procedimiento anterior tiene el gran inconveniente de que el canal se encuentra infrautilizado, hasta que el emisor no reciba un ACK no enviará ningún dato más, estando el canal desaprovechado todo ese tiempo. Una mejora de este método es el envío de una serie de datos numerados, de tal forma que en un sentido siempre se estén enviando datos (dato1, dato2, dato3...) y en el otro sentido se vayan recibiendo las confirmaciones (ACK1, ACK2, ACK3...). La cantidad de datos pendientes de ACK o NACK se establecerá según la memoria temporal del emisor.

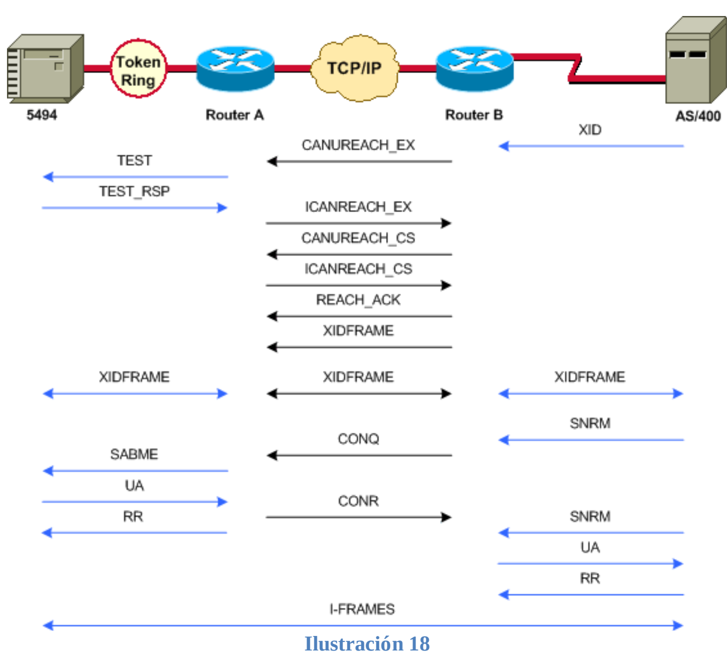



Ilustración 18

## *Preguntas propuestas*

1.- ¿Qué hechos trascendentales ha producido la ***revolución de la comunicación entre computadoras***?

2.- ¿A qué se refiere la ***utilización del sistema de transmisión***?

3.- ¿Qué debe tener un ***dispositivo*** para comunicarse?

4.- ¿Qué se requiere una vez establecida la ***interface***?

5.- ¿Cuáles son las convenciones para la ***administración de intercambios***?

6.- ¿Qué se requiere para las circunstancias donde los ***errores*** no pueden ser tolerados?

7.- ¿A qué se refiere los conceptos de ***DIRECCIONAMIENTO Y ENRUTAMIENTO***?

8.- ¿Qué es la técnica de ***RECUPERACIÓN***?

9.- ¿Qué involucra el ***FORMATO DEL MENSAJE***?

10.- Si el remitente de los datos desearía tener la seguridad de que sólo el destinatario recibirá sus datos y viceversa ¿Qué técnica usaría?

11.- ¿Qué requiere un sistema de comunicación de datos?

***Respuestas a las preguntas propuestas***

1.-

- No hay diferencia fundamental entre procesamiento de datos (computadoras) y comunicación de datos (equipos de conmutación y transmisión).
- No hay diferencia fundamental entre las comunicaciones de datos, voz y video.
- Las líneas entre computadoras de un solo procesador, computadoras con multiprocesadores, redes locales, redes metropolitanas y redes de gran alcance se han traslapado (puesto borrosas).

2.-

- Se refiere a la necesidad de hacer un uso eficiente de las facilidades de transmisión que son típicamente compartidas entre varios dispositivos de comunicación.
- Se usan varias técnicas (como multiplexaje) para asignar la capacidad total del medio de transmisión entre varios usuarios.
- Además se requiere varias técnicas de control de congestión para que el sistema se sobrecargue por excesiva demanda de los servicios de transmisión.

3.-

- Para comunicarse, un dispositivo debe tener una ***INTERFACE*** con el sistema de transmisión.

4.-

- Una vez que la interface esté establecida, se requiere de la ***GENERACIÓN DE SEÑALES*** para la comunicación.
- La propiedad de estas señales, tanto en forma como en intensidad, deben ser tales que ellas sean capaces de propagarse a través del medio de transmisión y de ser interpretables como datos en el receptor.
- No solamente las señales generadas deben conformar los requerimientos del sistema de transmisión y del receptor, sino que también debe haber alguna forma de ***SINCRONIZACIÓN*** entre el transmisor y el receptor.

- El receptor debe ser capaz de determinar cuándo una señal empieza a llegar y cuándo termina. También debe saber la duración de cada elemento de señal.

5.-

a) Si ambos dispositivos podrían transmitir simultáneamente o deben hacerlo por turnos
b) La cantidad de datos que debe ser enviado cada vez
c) El formato de los datos
d) Qué hacer si se presentan ciertas contingencias como errores.

6.-

- Se requiere ***DETECCIÓN Y CORRECCIÓN DE ERRORES***. Éste es usualmente el caso de sistemas de procesamiento de datos. Por ejemplo, en la transferencia del archivo de una computadora a otra, implemente no es aceptable que el contenido de ese archivo sea alterado accidentalmente.
- Además se requiere un ***CONTROL DE FLUJO*** para que la fuente no sobrecargue el medio ni el destino al enviar datos más rápido de lo que éstos puedan ser procesados y absorbidos.

7.-

- Cuando más de dos dispositivos comparten un medio de transmisión, el sistema debe ser informado por la fuente de la identidad de la estación destinataria.
- El sistema de transmisión debe asegurar que la estación de destino, y sólo esa estación, reciba los datos.
- Aún más, este sistema puede ser en sí mismo una red a través de la cual se pueda escoger varias trayectorias, y de las cuales se elige una ruta específica.

8.-

- Esta técnica es necesaria cuando un intercambio de información, tal como una transacción con una base de datos, es interrumpido por una falla en alguna parte del sistema.
- El objetivo de esta técnica es que el sistema pueda reasumir la actividad en el punto de la interrupción o al menos que restaure el estado de los sistemas involucrados, a la condición previa al inicio del intercambio de información.

9.-

- El ***FORMATO DEL MENSAJE*** involucra un acuerdo entre ambas partes, "***la forma de los datos***" que van a intercambiarse.
- Ambas partes deben usar el mismo código binario de caracteres.

10.-

- Proporcionar algún grado de ***PROTECCIÓN*** al sistema de comunicación de datos.

11.-

- Un sistema de comunicación de datos es tan complejo que no puede funcionar por sí mismo.
- Requiere capacidades de ***ADMINISTRACIÓN DEL SISTEMA*** para configurarlo, supervisar su estado, reaccionar ante fallas y sobrecargas y planear inteligentemente su crecimiento futuro.

Capítulo 3

# *MODELOS DE RED*

## 3.1. Modelo de referencia ISO/OSI

El modelo OSI (*Open Systems Interconnection*, interconexión de sistemas abiertos) fue un intento de la Organización Internacional de Normas (ISO) para la creación de un estándar que siguieran los diseñadores de nuevas redes.

El modelo OSI, patrocinado por la Comunidad Europea y más tarde, por el gobierno de los Estados Unidos, nunca llegó a tener la implantación esperada. Entre otros motivos, porque el modelo TCP/IP ya había sido aceptado por aquella época entre investigadores los cuales se resistieron a un cambio que, para la mayoría, era un cambio a peor.

Las bases que sustentan Internet son realmente sencillas y quizás esto ha sido la clave de su éxito; el modelo OSI, en cambio, fue tan ambicioso y complejo que terminó arrinconado en las estanterías de los laboratorios.

Se trata de un modelo teórico de referencia: únicamente explica lo que debe hacer cada componente de la red sin entrar en los detalles de implementación.

Según Gerardo Jiménez Rochabrum[1]. "El modelo OSI, define como los fabricantes de productos de hardware y software, pueden crear productos que funcionen con los productos de los fabricantes, sin necesidad de controladores especiales o equipamiento opcional".

La Tabla 5, muestra las 7 capas del modelo ISO/OSI. Las tres primeras capas se utilizan para enrutar, esto es, mover la información de unas redes a otras. En cambio, las capas superiores son exclusivas de los nodos origen y destino. La capa física está relacionada con el medio de transmisión. En el extremo opuesto se encuentra la capa de aplicación.

[1] *Gerardo Jiménez Rochabrum, "Redes y Cableado Estructurado". Empresa Editora RITISA. 1ra.Edicion. Pág. 92. Perú. 2005.*

**Tabla 5**

| Capa | Nivel | Función / Característica |
|---|---|---|
| **7** | **Aplicación** | Programas de aplicación que usa la red. |
| **6** | **Presentación** | Estandariza la forma en que se presentan los datos a las aplicaciones. |
| **5** | **Sesión** | Gestiona las conexiones entre aplicaciones cooperativas. |
| **4** | **Transporte** | Proporciona servicios de detección y corrección de errores. |
| **3** | **Red** | Gestiona conexiones a través de la red para las capas superiores. |
| **2** | **Enlace de datos** | Proporciona servicio de envío de datos a través del enlace físico. |
| **1** | **Físico** | Define las características físicas de la red material. |

Los creadores del modelo OSI consideraron que era 7 el número de capas que mejor se ajustaba a sus requisitos.

OSI ofrece un modo útil de realizar la interconexión y la interoperabilidad entre redes, su objetivo es promover la interconexión de sistemas abiertos.

Es la propuesta que hizo la ISO (International Standards Organization) para estandarizar la interconexión de sistemas abiertos.

Un sistema abierto se refiere a que es independiente de una arquitectura específica.

La Tabla 6, relaciona las capas con las principales tecnologías y protocolos que intervienen en cada una de las capas en una red.

**Tabla 6**

| Capa | Nivel | Tecnologías y Protocolos de Red |
|---|---|---|
| **7** | **Aplicación** | **DNS, FTP, HTTP, IMAP, IRC, NFS, NNTP, NTP, POP3, SMB/CIFS, SMTP, SNMP, SSH, TELNET, SIP.** |
| **6** | **Presentación** | **XML, ASN, MIME, SSL/TLS.** |
| **5** | **Sesión** | **NETBIOS, RPC.** |
| **4** | **Transporte** | **TCP, SCTP, SPX, UDP.** |
| **3** | **Red** | **IP, APPLE TALK, IPX, NETBEUI, X.25, ICMP, IGMP** |
| **2** | **Enlace de datos** | **ETHERNET, ATM, FRAME RELAY, HDLC, PPP, TOKEN RING, WI-FI, STP, ARP, RARP.** |
| **1** | **Física** | **Cable de par trenzado, cable coaxial, cable fibra óptica, microondas, radio.** |

La Ilustración 19, muestra el nivel o capa donde funcionan los equipos de red.




**Ilustración 19**

Según Alberto León-García, Indra Widjaja[2]. “El modelo de referencia OSI divide el proceso global de comunicación en funciones que son desempeñadas por varias capas. En cada capa, un proceso en una computadora desarrolla una conversación con un proceso paritario en la otra computadora.”

Cada capa añade algo nuevo a la comunicación, como vamos a ver ahora:

- **Capa física**. Se refiere a medio físico real en el que ocurre la comunicación. Este puede ser un cable CAT5 de cobre, un par de fibras ópticas, ondas de radio, o cualquier medio capaz de transmitir señales. Cables cortados, fibras partidas, e interferencias de RF constituyen, todos, problemas de capa física. Se encarga de la transmisión de bits por un medio de transmisión, ya sea un medio guiado (un cable) o un medio no guiado (inalámbrico). Esta capa define, entre otros aspectos, lo que transmite cada hilo de un cable, los tipos de conectores, el voltaje que representa un 1 y el que representa un 0. La capa física será diferente dependiendo del medio de transmisión (cable de fibra óptica, cable par trenzado, enlace vía satélite, etc.) No interpreta la información que está enviando: sólo transmite ceros y unos.
- **Capa de enlace de datos**. La comunicación en esta capa se define se define como de enlace-local porque todos los nodos conectados a esta capa se comunican directamente entre sí. En redes modeladas de acuerdo con Ethernet, los nodos se identifican por su dirección MAC (Control de Acceso al medio). Este es un número exclusivo de 48 bits asignado de fábrica a todo dispositivo de red. Envía tramas de datos entre hosts (o routers) de una misma red. Delimita las secuencias de bits que envía a la capa física, escribiendo ciertos códigos al comienzo y al final de cada trama. Esta capa fue diseñada originalmente para enlaces punto a punto, en los cuales hay que aplicar un control de flujo para el envío continuo de grandes cantidades de información. Para las redes de difusión (redes en las que muchas computadoras comparten un mismo medio de transmisión) fue necesario diseñar la llamada subcapa de

[2] *Alberto León-García, Indra Widjaja, “Redes de Comunicación”. Editorial Mc Graw Hill. Pág. 43. España. 2002.*

acceso al medio. Esta subcapa determina quién puede acceder al medio en cada momento y cómo sabe cada host que un mensaje es para él, por citar dos problemas que se resuelven a este nivel.

- **Capa de red**. Esta es la capa donde ocurre el enrutamiento. IP es el más común de la capa de red. Se encarga de transferir los paquetes desde la capa de enlace local a la de otras redes. Los enrutadores cumplen esta función en una red por medio de al menos dos interfaces de red, una en cada una de las redes que se va interconectar. Se encarga del encaminamiento de paquetes entre el origen y el destino, atravesando tantas redes intermedias como sean necesarias. Los mensajes se fragmentan en paquetes y cada uno de ellos se envía de forma independiente. Su misión es unificar redes heterogéneas: todos los host tendrán un identificador similar a nivel de la capa de red (en Internet son las direcciones IP) independientemente de las redes que tengan en capas inferiores (Token Ring con cable coaxial, Ethernet con cable de fibra óptica, enlace submarino, enlace por ondas, etc.).
- **Capa de transporte**. Provee un método para obtener un servicio particular en un nodo de red específico. El protocolo TCP garantiza que todos los datos lleguen a destino y se reorganicen y entreguen a la próxima capa en el orden apropiado. UDP es un protocolo no orientado a conexión comúnmente usado para señales de video y audio de flujo continuo. Únicamente se preocupa de la transmisión origen-destino. Podemos ver esta capa como una canalización fiable que une un proceso de un host con otro proceso de otro host. Un host puede tener varios procesos ejecutándose: uno para mensajería y otro para transferir archivos, por ejemplo. No se preocupa del camino intermedio que siguen los fragmentos de los mensajes. Integra control de flujo y control de errores, de forma que los datos lleguen correctamente de un extremo a otro.
- **Capa de sesión**. Maneja la sesión de comunicación lógica entre aplicaciones. NetBios y RPC son dos ejemplos de protocolo en ésta capa. Se encarga de iniciar y finalizar las comunicaciones. Además proporciona servicios mejorados a la capa de transporte como, por ejemplo, la creación de puntos de sincronismo para recuperar transferencias largas fallidas.

- **Capa de presentación**. Tienen que ver con representación de datos, antes de que lleguen a la aplicación. Esta incluye codificación MIME, compresión de datos, compresión de formato, ordenación de los bytes, etc. Codifica los datos que recibe de la capa de aplicación a un sistema convenido entre emisor y receptor, con el propósito de que tanto textos como números sean interpretados correctamente. Una posibilidad es codificar los textos según la tabla ASCII y los números en complemento a dos.
- **Capa de aplicación**. Es la capa con la que la mayoría de los usuarios tiene contacto y es el nivel en el que ocurre la comunicación humana. HTTP, FTP y STP son todos protocolos de la capa de aplicación. El usuario se ubica por encima de esta capa interactuando con la aplicación. Aquí se encuentran los protocolos y programas que utiliza el usuario para sus comunicaciones en red. Esta capa tendrá que ser adaptada para cada tipo de computador, de forma que sea posible el envío de un correo electrónico (u otros servicios) entre sistemas heterogéneos como Macintosh, Linux o Windows.

La Ilustración 20, muestra los protocolos más importantes y su relación en cada capa o nivel del modelo ISO / OSI.

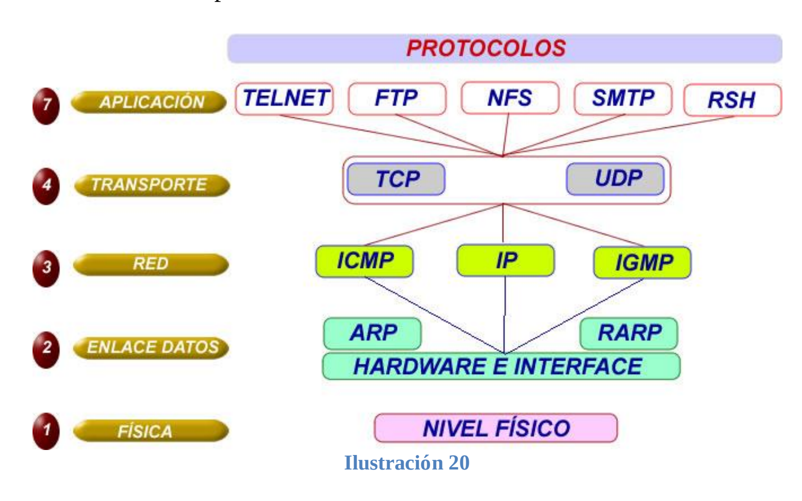



Ilustración 20

El modelo divide las redes en capas. Cada una de estas capas debe tener una función bien definida y relacionarse con sus capas inmediatas mediante unos interfaces también bien definidos. Esto debe permitir la sustitución de una de las capas sin afectar al resto, siempre y cuando no se varíen los interfaces que la relacionan con sus capas superior e inferior.

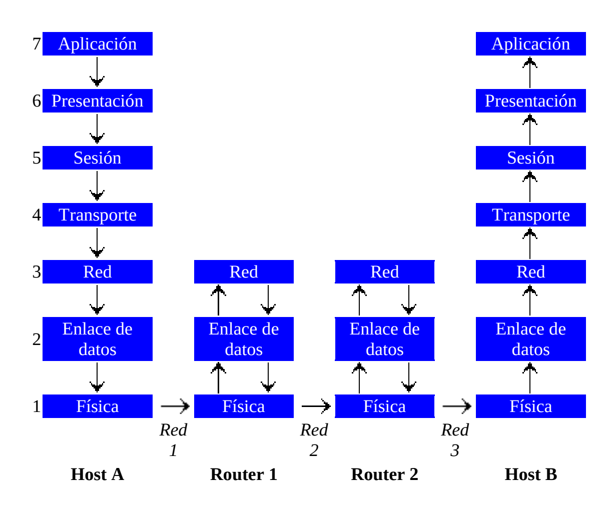



**Ilustración 21**

La Ilustración 21, muestra las 7 capas del modelo OSI. Las tres primeras capas se utilizan para *enrutar*, esto es, mover la información de unas redes a otras. En cambio, las capas superiores son exclusivas de los nodos origen y destino. La capa física está relacionada con el medio de transmisión (cableado concreto que utiliza cada red). En el extremo opuesto se encuentra la capa de aplicación: un programa de mensajería electrónica, por ejemplo. El usuario se situaría por encima de la capa 7.

La Ilustración 22, muestra el flujo de información entre capas.

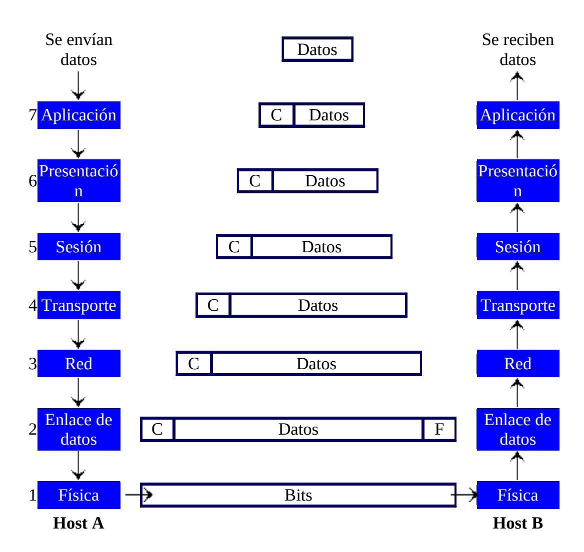



**Ilustración 22**

El host A es el nodo origen y el host B, el nodo destino. Nótese que estos papeles se intercambian continuamente en cualquier comunicación. Supongamos que mediante este modelo queremos enviar un mensaje al usuario del host B. El mensaje son los "datos" que se han dibujado por encima de la capa 7. Estos datos van descendiendo de capa en capa hasta llegar a la capa física del host A.

Cada capa añade un encabezado (C = cabecera) a los datos que recibe de la capa superior antes de enviárselos a su capa inferior. En la capa de enlace de datos se ha añadido también una serie de códigos al final de la secuencia (F = final) para delimitar no sólo el comienzo sino también el final de un paquete de datos.

La capa física no entiende de datos ni de códigos, únicamente envía una secuencia de bits por el medio de transmisión (un cable).

Estos bits llegarán, probablemente pasando por varios encaminadores intermedios, hasta la capa física del host destino. A medida que se van recibiendo secuencias de bits, se van pasando a las capas superiores.

Cada capa elimina su encabezado antes de pasarlo a una capa superior. Obsérvese que el mensaje que envía cada capa del host A a su capa inferior es idéntico al que recibe la capa equivalente del host B desde una capa inferior. Finalmente los datos llegarán a la capa de aplicación, serán interpretados y mostrados al usuario del host B.

Los paquetes de datos de cada capa suelen recibir nombres distintos. En la capa de enlace de datos se habla de *marcos* o *tramas*; en la capa de red, de *paquetes* o *datagramas*. En la capa de transporte, en ocasiones se utiliza el término *segmento*.

Cada capa se comunica con la capa equivalente de otro host (por ejemplo, la capa de red de un host *se entiende* con la capa de red de otro host). Sin embargo, como hemos visto, la comunicación realmente se realiza descendiendo capas en el host origen, transmitiendo por el medio físico y aumentando capas en el host destino. Cada capa añade algo nuevo a la comunicación,

Sin embargo, la idea de la división por capas del modelo OSI es realmente valiosa. Esta misma idea se aplica a todas las redes actuales, incluyendo Internet.

Como hemos comentado al principio, OSI es un modelo teórico general que da preferencia a un buen diseño en papel, antes que a la implementación de los protocolos.

## 3.2. Modelo TCP/IP

A diferencia del modelo OSI, el modelo TCP/IP no es un estándar internacional, y su definición varía. Sin embargo, es usado a menudo como un modelo práctico para entender y resolver fallas en redes Internet. La mayor parte de Internet usa TCP/IP, así que podemos plantear algunas premisas sobre las redes que las harán de más fácil comprensión.

El modelo TCP/IP se hizo justamente al revés: primero vinieron los protocolos y después, se pensó en sus especificaciones. De tal forma, que el modelo TCP/IP únicamente es aplicable para la pila de protocolos TCP/IP pero no es válido para nuevas redes.

En términos del modelo OSI, las capas cinco a siete quedan comprendidas en la capa superior (la Capa de Aplicación). Las primeras cuatro capas de ambos modelos son idénticas. Muchos ingenieros de redes consideran todo lo que está por encima de la capa cuatro como “sólo datos”, que van a variar de aplicación a aplicación. Ya que las primeras tres capas son interoperables para los equipos de casi todos los fabricantes, y la capa cuatro trabaja entre todos los anfitriones que usan TCP/IP, y todo lo que está por arriba de la capa cuatro es para aplicaciones específicas, este modelo simplificado funciona bien cuando se construyen o detectan fallas en redes TCP/IP.

Una manera de mirar al modelo TCP/IP es pensar en una persona que entrega una carta en un edificio de oficinas. Va a tener que interactuar primero con la calle (capa física), poner atención al tráfico de la misma (capa de enlace), doblar en los lugares correctos para conectarse con otras calles y arribar a la dirección correcta (capa Internet), ir al piso y oficina correcta (capa transporte) y finalmente encontrar el destinatario o recepcionista que puede recibir la carta (capa de aplicación). Una vez entregada la carta, el mensajero queda libre.

Las cinco capas pueden ser recordadas fácilmente usando la frase: Favor Entrar, Inmediatamente Tomar el Ascensor, para la secuencia de capas Física, Enlace de Datos, Internet, Transporte y Aplicación, o en inglés “Please Don’t Look In The Attic,” que se usa por “Physical / Data Link / Internet / Transport / Application”.

Internet no es un nuevo tipo de red física, sino un conjunto de tecnologías que permiten interconectar redes muy distintas entre sí.

Internet no es dependiente de la computadora ni del sistema operativo utilizado.

De esta manera, podemos transmitir información entre un servidor Unix y un computador que utilice Windows XP o entre plataformas completamente distintas como Macintosh, AMD, Alpha o Intel.

Es más, entre una computadora y otra generalmente existirán redes distintas: redes Ethernet, redes Token Ring e incluso enlaces vía satélite.

Como vemos, está claro que no podemos utilizar ningún protocolo que dependa de una arquitectura en particular. Lo que estamos buscando es un método de interconexión general que sea válido para cualquier plataforma, sistema operativo y tipo de red.

La familia de protocolos que se eligieron para permitir que Internet sea una red de redes es TCP/IP.

Nótese aquí que hablamos de familia de protocolos ya que son muchos los protocolos que la integran, aunque en ocasiones para simplificar hablemos sencillamente del protocolo TCP/IP.

El protocolo TCP/IP tiene que estar a un nivel superior del tipo de red empleado y funcionar de forma transparente en cualquier tipo de red. Y a un nivel inferior de los programas de aplicación (páginas WEB, correo electrónico, etc.) particulares de cada sistema operativo.

Todo esto nos sugiere el siguiente modelo de referencia:

El modelo TCP/IP tiene únicamente 3 capas:

- Capa de red
- Capa de transporte
- Capa de aplicación.

No tiene las capas de sesión ni de presentación que, por otro lado, estaban prácticamente vacías en el modelo OSI. Tampoco dice nada de las capas física y de enlace a datos.

Sin embargo, nosotros seguiremos un modelo de referencia fruto de combinar los modelos OSI y TCP/IP.

Se trata del modelo real que se está utilizando actualmente en las redes TCP/IP.

La Tabla 7, refleja las 5 capas de nuestro modelo.

**Tabla 7**

| Capa | Nivel | Tecnologías y Protocolos de Red |
|---|---|---|
| **5** | **Aplicación** | **DNS, FTP, HTTP, IMAP, IRC, NFS, NNTP, NTP, POP3, SMB/CIFS, SMTP, SNMP, SSH, TELNET, SIP. XML, ASN, MIME, SSL/TLS. NETBIOS.** |
| **4** | **Transporte** | **TCP, SCTP, SPX, UDP.** |
| **3** | **Red** | **IP, APPLE TALK, IPX, NETBEUI, X.25.** |
| **2** | **Enlace de datos** | **ETHERNET, ATM, FRAME RELAY, HDLC, PPP, TOKEN RING, WI-FI, STP.** |
| **1** | **Física** | **Cable de par trenzado, cable coaxial, cable fibra óptica, microondas, radio.** |

El nivel más bajo es la ***capa física***. Aquí nos referimos al medio físico por el cual se transmite la información. Generalmente será un cable aunque no se descarta cualquier otro medio de transmisión como ondas o enlaces vía satélite.

La ***capa de enlace de datos*** (acceso a la red) determina la manera en que las estaciones (computadoras) envían y reciben la información a través del soporte físico proporcionado por la capa anterior. Es decir, una vez que tenemos un cable, ¿cómo se transmite la información por ese cable? ¿Cuándo puede una estación transmitir? ¿Tiene que esperar algún turno o transmite sin más? ¿Cómo sabe una estación que un mensaje es para ella? Pues bien, son todas estas cuestiones las que resuelve esta capa.

Las dos capas anteriores quedan a un nivel inferior del protocolo TCP/IP, es decir, no forman parte de este protocolo.

La ***capa de red*** define la forma en que un mensaje se transmite a través de distintos tipos de redes hasta llegar a su destino. El principal protocolo de esta capa es el IP aunque también se encuentran a este nivel los protocolos ARP, ICMP e IGMP. Esta capa proporciona el direccionamiento IP y determina la ruta óptima a través de los

encaminadores (routers) que debe seguir un paquete desde el origen al destino.

La ***capa de transporte*** (protocolos TCP, SCTP, SPX, UDP) ya no se preocupa de la ruta que siguen los mensajes hasta llegar a su destino. Sencillamente, considera que la comunicación extremo a extremo está establecida y la utiliza. Además añade la noción de puertos.

La ***capa de aplicación*** utiliza una familia de tecnologías y protocolos de red (DNS, FTP, HTTP, IMAP, IRC, NFS, NNTP, NTP, POP3, SMB/CIFS, SMTP, SNMP, SSH, TELNET, SIP. XML, ASN, MIME, SSL/TLS. NETBIOS.).

## *Preguntas propuestas*

1.- ¿El modelo OSI es una arquitectura en particular?

2.- ¿El nivel físico que cuestiones define?

3.- ¿Cuál es el propósito del nivel de enlace?

4.- ¿Qué determina el nivel de red?

5.- ¿Qué servicios provee el nivel de transporte?

6.- ¿Qué servicios provee el nivel de sesión?

7.- ¿Qué funciones provee el nivel de presentación?

8.- ¿Qué define el nivel de aplicación?

9.- ¿Cuál es el objetivo de los protocolos TCP/IP?

10.- ¿Cuáles son los protocolos a nivel de transporte?

11.- ¿Cuáles son las diferencias entre el modelo ISO/OSI y TCP/IP?

## *Respuestas a las preguntas propuestas*

1.-

- En realidad no es una arquitectura particular, porque no especifica los detalles de los niveles, sino que los estándares de ISO existen para cada nivel.

2.-

- Las cuestiones de: voltajes, duración de un bit, establecimiento de una conexión, número de polos en un enchufe, etc.

3.-

- El propósito de este nivel es convertir el medio de transmisión crudo en uno que esté libre de errores de transmisión.
- El remitente parte los datos de input en marcos de datos (algunos cientos de bytes) y procesa los marcos de acuse.
- Este nivel maneja los marcos perdidos, dañados, o duplicados.
- Regula la velocidad del tráfico.
- En una red de broadcast, un subnivel (el subnivel de acceso medio, o medium access sublayer) controla el acceso al canal compartido.

4.-

- Determina el ruteo de los paquetes desde sus fuentes a sus destinos, manejando la congestión a la vez.
- Se incorpora la función de contabilidad.

5.-

- Es el primer nivel que se comunica directamente con su par en el destino (los de abajo son de computador a computador).
- Provee varios tipos de servicio (por ejemplo, un canal punto a punto sin errores).
- Podría abrir conexiones múltiples de red para proveer capacidad alta.
- Se puede usar el encabezamiento de transporte para distinguir entre los mensajes de conexiones múltiples entrando en un computador.
- Provee el control de flujo entre los hosts.

6.-

- Parecido al nivel de transporte, pero provee servicios adicionales.
- Por ejemplo, puede manejar tokens (objetos abstractos y únicos) para controlar las acciones de participantes o puede hacer checkpoints (puntos de recuerdo) en las transferencias de datos.

7.-

- Provee funciones comunes a muchas aplicaciones tales como traducciones entre juegos de caracteres, códigos de números, etc.

8.-

- Define los protocolos usados por las aplicaciones individuales, como e-mail, telnet, ftp, etc.

9.-

- Tiene como objetivos la conexión de redes múltiples y la capacidad de mantener conexiones aun cuando una parte de la subred esté perdida.
- La red es packet - switched y está basada en un nivel de internet sin conexiones. Los niveles físico y de enlace (que juntos se llaman el "nivel de host a red" aquí) no son definidos en esta arquitectura.
- Los hosts pueden introducir paquetes en la red, los cuales viajan independientemente al destino. No hay garantías de entrega ni de orden.
- Este nivel define el Internet Protocol (IP), que provee el ruteo y control de congestión.

10.-

- Transmission Control Protocol (TCP). Provee una conexión confiable que permite la entrega sin errores de un flujo de bytes desde una máquina a alguna otra en la internet. Parte el flujo en mensajes discretos y lo monta de nuevo en el destino. Maneja el control de flujo.
- User Datagram Protocol (UDP). Es un protocolo no confiable y sin conexión para la entrega de mensajes discretos. Se pueden construir otros protocolos de aplicación sobre UDP. También se

usa UDP cuando la entrega rápida es más importante que la entrega garantizada.

11.-

- OSI define claramente las diferencias entre los servicios, las interfaces, y los protocolos.
    - Servicio: lo que un nivel hace.
    - Interfaz: cómo se pueden accesar los servicios.
    - Protocolo: la implementación de los servicios
- TCP/IP no tiene esta clara separación.
- OSI fue definido antes de implementar los protocolos, los diseñadores no tenían mucha experiencia con donde se debieran ubicar las funcionalidades y algunas otras faltan. Por ejemplo, OSI originalmente no tiene ningún apoyo para broadcast.
- El modelo de TCP/IP fue definido después de los protocolos y se adecúan perfectamente. Pero no otras pilas de protocolos.
- OSI no tuvo éxito debido a:
    - Mal momento de introducción: insuficiente tiempo entre las investigaciones y el desarrollo del mercado a gran escala para lograr la estandarización.
    - Mala tecnología: OSI es complejo, es dominado por una mentalidad de telecomunicaciones sin pensar en computadores, carece de servicios sin conexión, etc.
    - Malas implementaciones.
    - Malas políticas: investigadores y programadores contra los ministerios de telecomunicación
- Sin embargo, OSI es un buen modelo (no los protocolos).
- TCP/IP es un buen conjunto de protocolos, pero el modelo no es general.

Capítulo 4

# *CAPA FISICA*

## 4.1. Medios de transmisión

La capa física determina el soporte físico o medio de transmisión por el cual se transmiten los datos. Estos medios de transmisión se clasifican en *guiados* y *no guiados*. Los primeros son aquellos que utilizan un medio sólido (un cable) para la transmisión. Los medios no guiados utilizan el aire para transportar los datos, son los medios inalámbricos.

Los medios guiados:

**Cable par trenzado,** El par trenzado es similar al cable telefónico, sin embargo consta de 8 hilos y utiliza unos conectores un poco más anchos. Dependiendo del número de trenzas por unidad de longitud, los cables de par trenzado se clasifican en categorías. A mayor número de trenzas, se obtiene una mayor velocidad de transferencia.

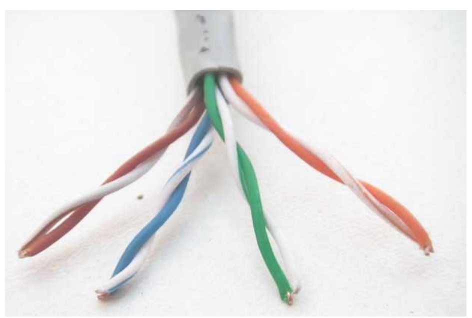
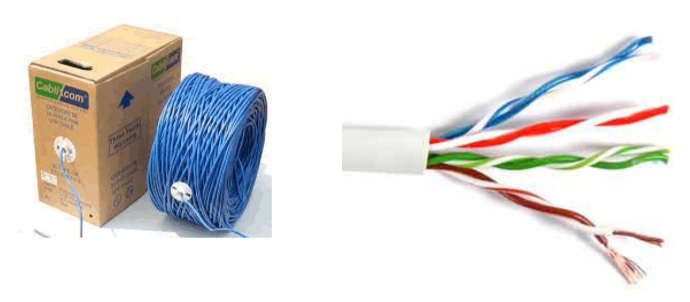


**Ilustración 23**

- Categoría 3, hasta 16 Mbps
- Categoría 4, hasta 20 Mbps
- Categoría 5 y Categoría 5e, hasta 100 Mbps
- Categoría 6, hasta 1 Gbps y más

Los cables par trenzado pueden ser a su vez de dos tipos:

- UTP (*Unshielded Twisted Pair*, par trenzado no apantallado)



- STP (*Shielded Twisted Pair*, par trenzado apantallado)

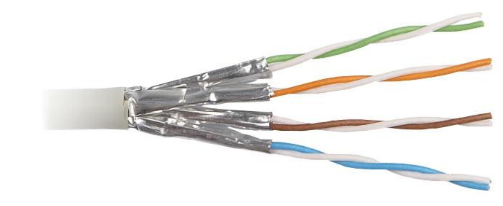
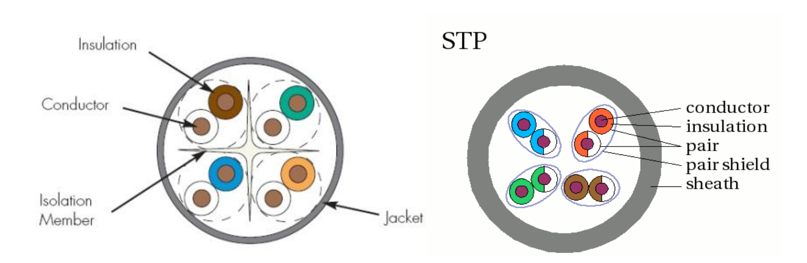


**Ilustración 24**




Los cables UTP son los más utilizados debido a su bajo costo y facilidad de instalación. Los cables STP están embutidos en una malla metálica que reduce las interferencias y mejora las características de la transmisión. Sin embargo, tienen un costo elevado y al ser más gruesos son más complicados de instalar.

El cableado que se utiliza en la actualidad es UTP CAT5.

El cableado CAT6 es demasiado nuevo y es difícil encontrarlo en el mercado.

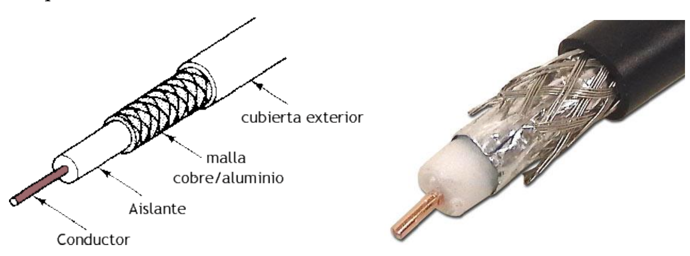
Los cables STP se utilizan únicamente para instalaciones muy puntuales que requieran una calidad de transmisión muy alta.

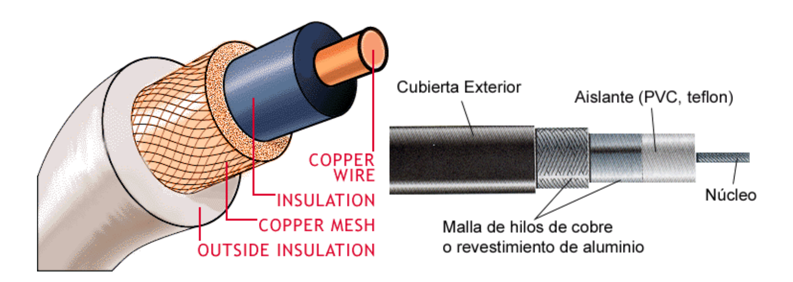
Los segmentos de cable van desde cada una de las estaciones hasta un aparato denominado *hub* (concentrador) o switch (conmutador), formando una topología de estrella.



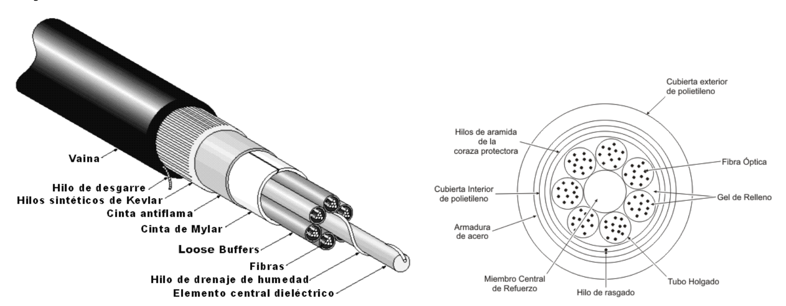


**Cable coaxial,** El cable coaxial es similar al cable utilizado en las antenas de televisión: un hilo de cobre en la parte central rodeado por una malla y separados ambos elementos conductores por un cilindro de plástico. Las redes que utilizan este cable requieren que los adaptadores tengan un conector apropiado, los computadores forman una fila y se coloca un segmento de cable entre cada computador y el siguiente. En los extremos hay que colocar un terminador, que no es más que una resistencia de 50 ohmios.






**Cable fibra óptica,** En los cables de fibra óptica la información se transmite en forma de pulsos de luz. En un extremo del cable se coloca un diodo luminoso (LED) o bien un láser, que puede emitir luz, y en el otro extremo se sitúa un detector de luz.




Curiosamente y a pesar de este sencillo funcionamiento, mediante los cables de fibra óptica se llegan a alcanzar velocidades de varios Gbps. Sin embargo, su instalación y mantenimiento tiene un costo elevado y solamente son utilizados para redes troncales con mucho tráfico.



Los cables de fibra óptica son el medio de transmisión elegido para las redes de *cable*. Se pretende que este *cable* pueda transmitir televisión, radio, Internet y teléfono.

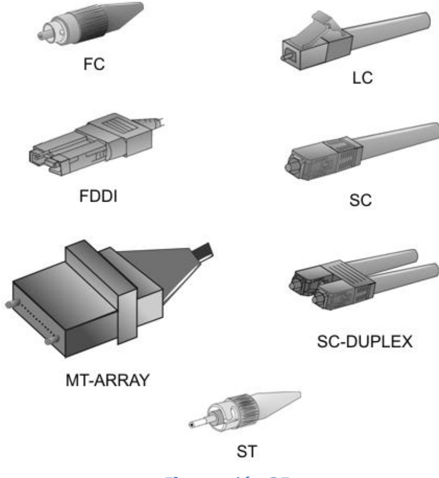
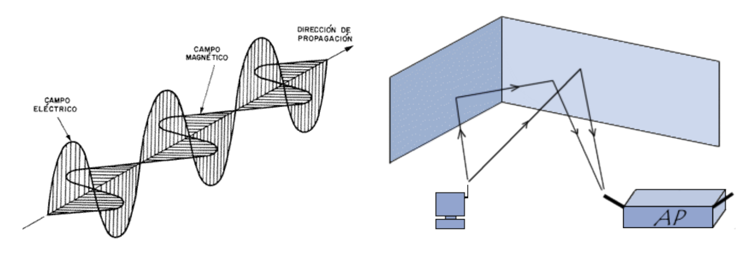



Ilustración 25

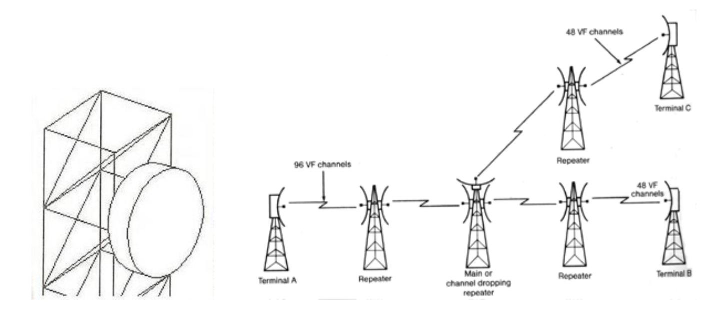
***Entre los medios no guiados se encuentran:***

**Ondas de radio**. Son capaces de recorrer grandes distancias, atravesando edificios incluso. Son ondas omnidireccionales, se propagan en todas las direcciones. Su mayor problema son las interferencias entre usuarios.

Las ondas electromagnéticas no necesitan de un medio material para propagarse.



**Microondas**. Estas ondas viajan en línea recta, por lo que emisor y receptor deben estar alineados cuidadosamente. Tienen dificultades para atravesar edificios. Debido a la propia curvatura de la tierra, la distancia entre dos repetidores no debe exceder de unos 80 Kms. de distancia.




**Infrarrojos**. Son ondas direccionales incapaces de atravesar objetos sólidos (paredes, por ejemplo) que están indicadas para transmisiones de corta distancia.

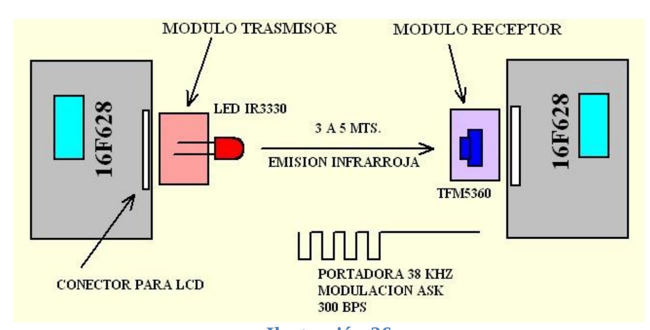



Ilustración 26



Ilustración 27

**Ondas de luz**. Las ondas láser son unidireccionales.

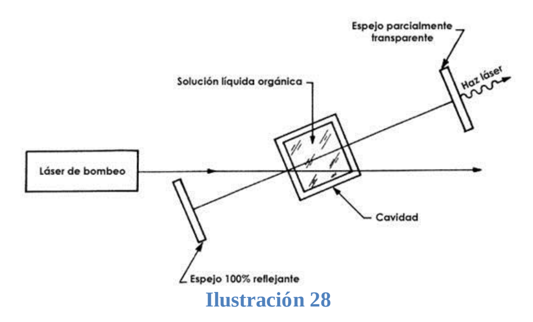



Ilustración 28

Se pueden utilizar para comunicar dos edificios próximos instalando en cada uno de ellos un emisor láser y un foto detector.

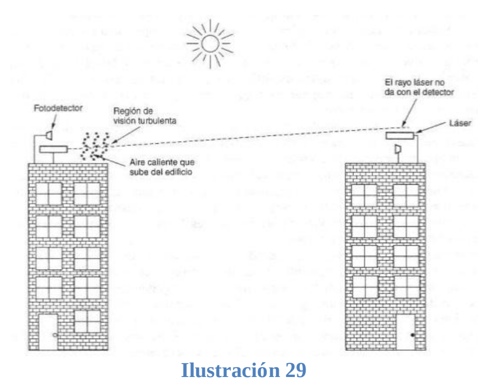



Ilustración 29

## 4.2. Instalación de cableado

### *Cable coaxial*

El cable coaxial fue creado en la década de los 30, y es un cable utilizado para transportar señales eléctricas de alta frecuencia que posee dos conductores concéntricos, uno central, llamado vivo, encargado de llevar la información, y uno exterior, de aspecto tubular, llamado malla o blindaje, que sirve como referencia de tierra y retorno de las corrientes. Entre ambos se encuentra una capa aislante llamada dieléctrico, de cuyas características dependerá principalmente la calidad del cable. Todo el conjunto suele estar protegido por una cubierta aislante.

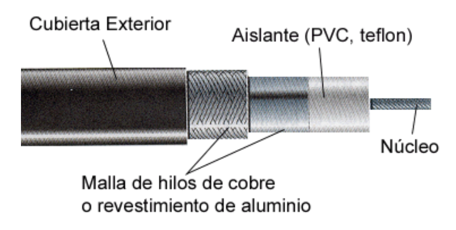



Ilustración 30

El conductor central puede estar constituido por un alambre sólido o por varios hilos retorcidos de cobre; mientras que el exterior puede ser una malla trenzada, una lámina enrollada o un tubo corrugado de cobre o aluminio. En este último caso resultará un cable semirrígido.

El cable coaxial es más resistente a interferencias y atenuación que el cable de par trenzado, por esto hubo un tiempo que fue el más usado.

La malla de hilos absorbe las señales electrónicas perdidas, de forma que no afecten a los datos que se envían a través del cable interno. Por esta razón, el cable coaxial es una buena opción para grandes distancias y para soportar de forma fiable grandes cantidades de datos con un sistema sencillo.

En los cables coaxiales los campos debidos a las corrientes que circulan por el interno y externo se anulan mutuamente.

La característica principal de la familia RG-58 es el núcleo central de cobre. Tipos:

- RG-58/U: Núcleo de cobre sólido.
- RG-58 A/U: Núcleo de hilos trenzados.
- RG-59: Transmisión en banda ancha (TV).
- RG-6: Mayor diámetro que el RG-59 y considerado para frecuencias más altas que este, pero también utilizado para transmisiones de banda ancha.
- RG-62: Redes ARCnet.



Ilustración 31

## Estándares

La mayoría de los cables coaxiales tienen una impedancia característica de 50, 52, 75, o 93 Ω. La industria de RF usa nombres de tipo estándar para cables coaxiales.

En las conexiones de televisión (por cable, satélite o antena), los cables RG-6 son los más comúnmente usados para el empleo en el hogar, y la mayoría de conexiones fuera de Europa es por conectores F.



Ilustración 32

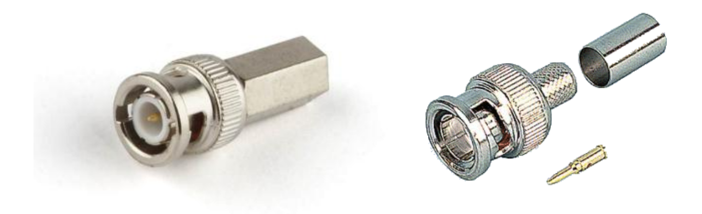
## Tipos de cable coaxial RG

Tabla 8

| Tipo | Impedancia [Ω] | Núcleo |
|---|---|---|
| **RG-6/U** | 75 | 1.0 mm |
| **RG-6/UQ** | 75 | |
| **RG-8/U** | 50 | 2.17 mm |
| **RG-9/U** | 51 | |
| **RG-11/U** | 75 | 1.63 mm |
| **RG-58** | 50 | 0.9 mm |
| **RG-59** | 75 | 0.81 mm |
| **RG-62/U** | 92 | |
| **RG-62A** | 93 | |
| **RG-174/U** | 50 | 0.48 mm |
| **RG-178/U** | 50 | 7x0.1 mm Ag pltd Cu clad Steel |
| **RG-179/U** | 75 | 7x0.1 mm Ag pltd Cu |
| **RG-213/U** | 50 | 7x0.0296 en Cu |
| **RG-214/U** | 50 | 7x0.0296 en |
| **RG-218** | 50 | 0.195 en Cu |
| **RG-223** | 50 | 2.74mm |
| **RG-316/U** | 50 | 7x0.0067 in |

## Conectores para cable coaxial

### *Conector BNC*



Ensamblaje del conector **BNC**:



Ilustración 33

### *Conector PL-259*





Ensamblaje del conector **PL-259**:



Ilustración 34

### *Cable par trenzado*

El cable de par trenzado es una forma de conexión en la que dos conductores eléctricos aislados son entrelazados para tener menores interferencias y aumentar la potencia y disminuir la diafonía de los cables adyacentes.

El entrelazado de los cables disminuye la interferencia debido a que el área de bucle entre los cables, la cual determina el acoplamiento eléctrico en la señal, se ve aumentada.

En la operación de balanceado de pares, los dos cables suelen llevar señales paralelas y adyacentes (modo diferencial), las cuales son combinadas mediante sustracción en el destino.

El ruido de los dos cables se aumenta mutuamente en esta sustracción debido a que ambos cables están expuestos a EMI similares.

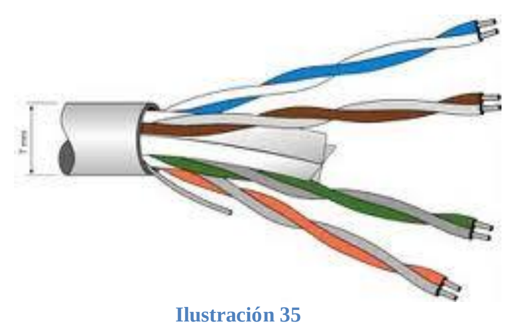


Ilustración 35

## Estándar para el cableado de telecomunicaciones de edificios comerciales

Estándar de la Industria Americana:

- EIA/TIA – 568 – Julio 1991
- EIA/TIA – 568A – Octubre 1995
- EIA/TIA – 568B – 1998/1999

Provee una estructura común para el diseño e instalaciones de cables de telecomunicaciones y hardware de conectividad en los edificios comerciales.

### Norma 568-A

1) Blanco-Verde
2) verde
3) Blanco-Naranja
4) azul
5) Blanco-Azul
6) Naranja
7) Blanco-Marrón
8) Marrón

### Norma 568-B

1) Blanco-Naranja
2) Naranja
3) Blanco-Verde
4) Azul
5) Blanco-Azul
6) Verde
7) Blanco-Marrón
8) Marrón

## Tipos de conexión

Los cables UTP forman los segmentos de Ethernet y pueden ser cables rectos o cables cruzados dependiendo de su utilización.

### *Cable par trenzado directo (pin a pin)*

Estos cables conectan un concentrador a un nodo de red (Hub, Nodo). Cada extremo debe seguir la misma norma (EIA/TIA 568A o 568B) de configuración. La razón es que el concentrador es el que realiza el cruce de la señal.

Los conectores de cada extremo siguen el mismo esquema de colores.

Estos cables se utilizan para unir:

- computador con hub.
- 2 hubs (utilizando el puerto *uplink* de uno de ellos y un puerto normal del otro).




Ilustración 36

***Cable par trenzado cruzado (cross-over)***

Este tipo de cable se utiliza cuando se conectan elementos del mismo tipo, dos enrutadores, dos concentradores. También se utiliza cuando conectamos 2 computadores directamente, sin que haya enrutadores o algún elemento de por medio.

Para hacer un cable cruzado se usará una de las normas en uno de los extremos del cable y la otra norma en el otro extremo.

Lo que estamos haciendo es cruzar los pines de transmisión (Tx+ y Tx-) de un extremo con los pines de recepción (Rx+ y Rx-) del otro.

De acuerdo al siguiente esquema:

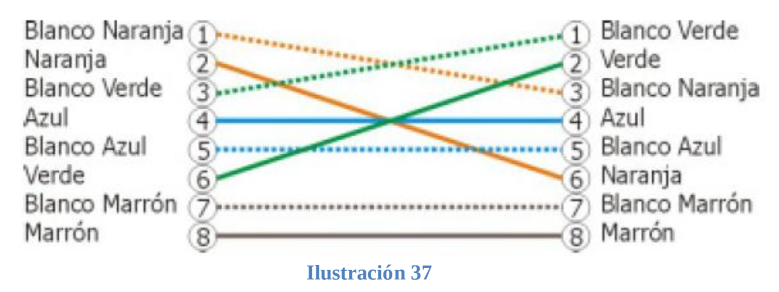



Ilustración 37

Estos cables se utilizan para unir:

- 2 computadores sin necesidad de hub (el cable va de una tarjeta de red a la otra).
- 2 hubs (sin utilizar el puerto *uplink* de ninguno de ellos o utilizando el puerto *uplink* en ambos).

***Conectores para cable de par trenzado***

***Conector RJ-45 / MACHO***

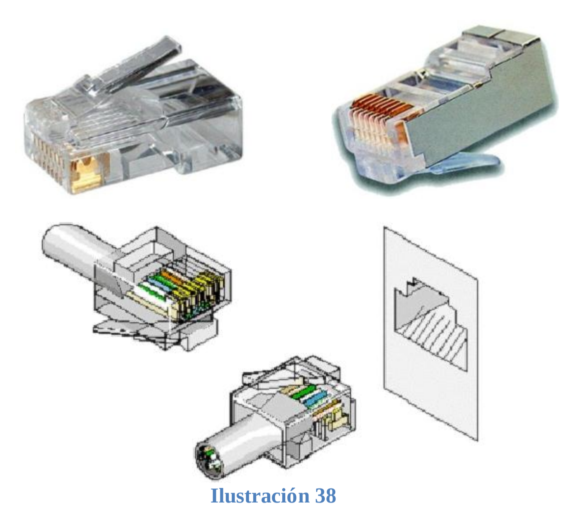


Ilustración 38

***Conector RJ-45 / HEMBRA***

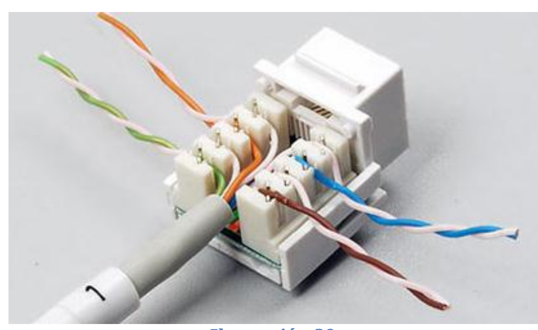


Ilustración 39

## 4.3. Comparación entre *hub* y *switch*

Un *hub* pertenece a la capa física: se puede considerar como una forma de interconectar unos cables con otros. Un *switch*, en cambio, trabaja en la capa de acceso a la red (son la versión moderna de los puentes o *bridges*) pero también puede tratarse como un sistema de interconexión de cables, eso sí, con cierta *inteligencia*. Los puestos de la red no tienen forma de conocer si las tramas Ethernet que están recibiendo proceden de un hub, switch o han pasado directamente mediante un cable par trenzado cruzado. Estos dispositivos no requieren ninguna configuración software: únicamente con enchufarlos ya comienzan a operar.

***Nota:*** *Un router (encaminador) pertenece a la capa de red. Trabaja con direcciones IP. Se utiliza para interconectar redes y requiere una configuración. Podemos averiguar los routers que atraviesan nuestros datagramas IP mediante el comando* ***Tracert****.*

Un ***hub o concentrador*** es el punto central desde el cual parten los cables de par trenzado hasta las distintos puestos de la red, siguiendo una topología de estrella. Se caracterizan por el número de puertos y las velocidades que soportan. Por ejemplo, son habituales los hub 10/100 de 8 puertos.

- Los hub *difunden* la información que reciben desde un puerto por todos los demás (su comportamiento es similar al de un ladrón eléctrico).
- Todas sus ramas funcionan a la *misma velocidad*. Esto es, si mezclamos tarjetas de red de 10/100 Mbps y 10 Mbps en un mismo hub, todas las ramas del hub funcionarán a la velocidad menor (10 Mbps).
- Es habitual que contengan un *diodo luminoso* para indicar si se ha producido una colisión. Además, los concentradores disponen de tantas lucecitas (LED) como puertos para informar de las ramas que tienen señal.




**Ilustración 40**

Un ***switch o conmutador*** es un hub mejorado: tiene las mismas posibilidades de interconexión que un hub (al igual que un hub, no impone ninguna restricción de acceso entre los computadores conectados a sus puertos). Sin embargo se comporta de un modo más eficiente reduciendo el tráfico en las redes y el número de colisiones.

- Un switch *no difunde* las tramas Ethernet por todos los puertos, sino que las retransmite sólo por los puertos necesarios. Por ejemplo, si tenemos un computador A en el puerto 3, un computador B en el puerto 5 y otro computador C en el 6, y enviamos un mensaje desde A hasta C, el mensaje lo recibirá el switch por el puerto 3 y sólo lo reenviará por el puerto 6 (un hub lo hubiese reenviado por todos sus puertos).
- Cada puerto tiene un *buffer* o memoria intermedia para almacenar tramas Ethernet.
- Puede trabajar con *velocidades distintas* en sus ramas (*autosensing*): unas ramas pueden ir a 10 Mbps y otras a 100 Mbps.
- Suelen contener 3 *diodos luminosos* para cada puerto: uno indica si hay señal (link), otro la velocidad de la rama (si está encendido es 100 Mbps, apagado es 10 Mbps) y el último se enciende si se ha producido una colisión en esa rama.




**Ilustración 41**




**Ilustración 42**

¿Cómo sabe un switch los computadores que tiene en cada rama?

Lo averigua de forma automática mediante *aprendizaje*. Los conmutadores contienen una tabla dinámica de direcciones físicas y números de puerto. Nada más enchufar el switch esta tabla se

encuentra vacía. Un procesador analiza las tramas Ethernet entrantes y busca la dirección física de destino en su tabla. Si la encuentra, únicamente reenviará la trama por el puerto indicado. Si por el contrario no la encuentra, no le quedará más remedio que actuar como un hub y difundirla por todas sus ramas.

Las tramas Ethernet contienen un campo con la dirección física de origen que puede ser utilizado por el switch para agregar una entrada a su tabla basándose en el número de puerto por el que ha recibido la trama. A medida que el tráfico se incrementa en la red, la tabla se va construyendo de forma dinámica. Para evitar que la información quede desactualizada (si se cambia un computador de sitio, por ejemplo) las entradas de la tabla desaparecerán cuando agoten su tiempo de vida (TTL), expresado en segundos.

***Dominios de colisión***

Un *dominio de colisión* es un segmento del cableado de la red que comparte las mismas colisiones. Cada vez que se produzca una colisión dentro de un mismo dominio de colisión, afectará a todos los computadores conectados a ese segmento pero no a los computadores pertenecientes a otros dominios de colisión.

Todas las ramas de un *hub* forman un mismo dominio de colisión (las colisiones se retransmiten por todos los puertos del hub). Cada rama de un *switch* constituye un dominio de colisiones distinto (las colisiones no se retransmiten por los puertos del switch). Este es el motivo por el cual la utilización de conmutadores reduce el número de colisiones y mejora la eficiencia de las redes. El ancho de banda disponible se reparte entre todos los computadores conectados a un mismo dominio de colisión.

***Nota:*** *Podemos indicar un número aproximado de 25-30 como medida máxima de computadores que se pueden conectar dentro de un mismo dominio de colisión. Sin embargo, este número dependerá en gran medida del tráfico de la red. En redes con mucho tráfico se debe tratar de reducir el número de computadores por dominio de colisión lo más posible mediante la creación de distintos dominios de colisión conectados por switches o mediante la creación de distintas subredes conectadas por routers.*

¿Qué instalar hubs o switches?

- Siempre que el presupuesto lo permita *elegiremos un switch antes que un hub*.

- Si nuestra red tiene un elevado número de computadores (hay que utilizar varios concentradores enlazados) pero sólo nos podemos permitir un switch, éste lo colocaremos en *el lugar de la red con más tráfico* (habitualmente será el concentrador situado en el centro de la estrella de estrellas o bien, aquél que contenga a los servidores). En el resto de las posiciones colocaremos hubs. El esquema descrito se utiliza a menudo: un hub en cada departamento y un switch para interconectar los departamentos con los servidores. Desde luego, lo ideal sería colocar switches en todas las posiciones.
- Además de la mejora en eficiencia que supone utilizar un switch frente a un hub, debemos considerar también el *aumento de seguridad*: si en un computador conectado a un switch se instala, con fines nada éticos, un programa para escuchar el tráfico de la red (*sniffer*), el atacante sólo recibirá las tramas Ethernet que corresponden a ese computador pero no las tramas de otros computadores que podrían contener contraseñas ajenas.

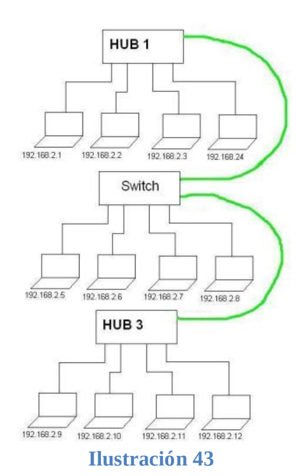



**Ilustración 43**

## 4.4. Interconexión de hub

Los concentradores incluyen un puerto diferenciado, etiquetado con el nombre "uplink" o "cascade", para facilitar su interconexión con otros hub. El puerto "uplink" de un hub se conecta mediante un cable par trenzado directo hasta un puerto cualquiera (que no sea el "uplink") del otro hub. Si ninguno de los dos hub tuviese el puerto "uplink" libre todavía se podrían interconectar utilizando un cable par trenzado cruzado.

***Nota:*** *Todo lo que se comenta en este apartado referente a hub (concentradores) es equivalente para los switches (conmutadores).*

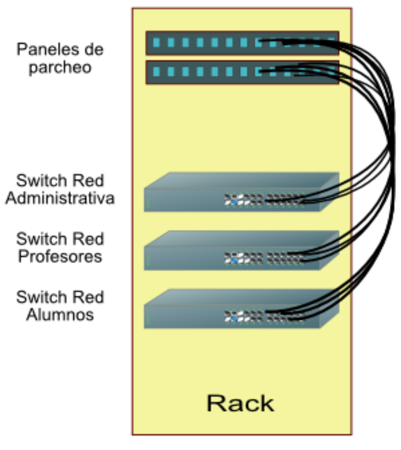



**Ilustración 44**

¿Dónde se encuentra el puerto "uplink"? Dependiendo de los fabricantes se suele dar una de estas dos situaciones:

- El hub es de *n* puertos pero tiene *n+1* conectores, uno de ellos tiene una marca especial. Por ejemplo, son habituales los hub que tienen 9 conectores: 7 puertos normales y un puerto mixto con dos conectores contiguos los cuales no se pueden utilizar simultáneamente. El número máximo de cables que podemos conectar es de 8, quedando un conector vacío (el marcado como "uplink" o el que tiene justo a su lado).
- El hub es de *n* puertos y tiene *n* conectores, uno de ellos tiene una marca especial. Mediante un botón conmutamos la función del conector diferenciado entre "uplink" y puerto normal. Las prestaciones son las mismas que en el caso anterior. Este diseño es habitual de los hub del fabricante 3COM.

¿Cómo enlazar unos hub con otros? Los diseños más habituales son los dos siguientes, aunque se suelen combinar:

- *Hub encadenados*. Un hub se va conectando con el siguiente formando una cadena. No es conveniente conectar de esta forma más de 3 hub puesto que el rendimiento de la red disminuirá considerablemente (las señales tardan en pasar desde el primer hub de la cadena hasta el último).

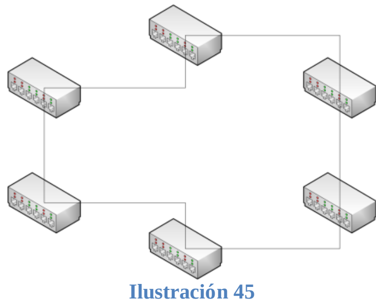


Ilustración 45

- *Hub en estrella*. Se coloca un hub en el centro y de éste se tiran cables hasta el resto de los hub. Con esta solución se consiguen velocidades más altas en la red aunque el cableado es más costoso.

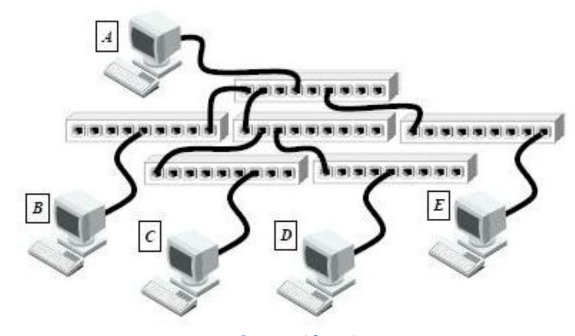



Ilustración 46

## 4.5. Cableado estructurado

Un sistema de cableado estructurado es la infraestructura de cable que cumple una serie de normas y que está destinada a transportar las señales de un emisor hasta el correspondiente receptor, es decir que su principal objetivo es proveer un sistema total de transporte de información a través de un mismo tipo de cable (medio común).

Esta instalación se realiza de una manera ordenada y planeada lo cual ayuda a que la señal no se degrade en la transmisión y asimismo garantizar el desempeño de la red. El cableado estructurado se utiliza para trasmitir voz, datos, imágenes, dispositivos de control, de seguridad, detección de incendios, entre otros.

Dicho sistema es considerado como un medio físico y pasivo para las redes de área local (LAN) de cualquier edificio en el cual se busca independencia con las tecnologías usadas, el tipo de arquitectura de red o los protocolos empleados. Por lo tanto el sistema es transparente ante redes Ethernet, Token Ring, ATM, RDSI o aplicaciones de voz, de control o detección. Es por esta razón que se puede decir que es un sistema flexible ya que tiene la capacidad de aceptar nuevas tecnologías solo teniéndose que cambiar los adaptadores electrónicos en cada uno de los extremos del sistema. La gran ventaja de esta característica es que el sistema de cableado se adaptará a las aplicaciones futuras por lo que asegura su vigencia por muchos años.

Cabe resaltar que la garantía mínima de un sistema de este tipo es mínimo de 20 años, lo que lo hace el componente de red de mayor duración y por ello requiere de atención especial.

Por otro lado, al ser una instalación planificada y ordenada, se aplican diversas formas de etiquetado de los numerosos elementos a fin de localizar de manera eficiente su ubicación física en la infraestructura. A pesar de que no existe un estándar de la forma cómo se debe etiquetar los componentes, dos características fundamentales son: que cada componente debe tener una etiqueta única para evitar ser confundido con otros elementos y que toda etiqueta debe ser legible y permanente.

Los componentes que deberían ser etiquetados son: espacios, ductos o conductos, cables, hardware y sistema de puesta a tierra.

Asimismo se sugiere llevar un registro de toda esta información ya que luego serán de valiosa ayuda para la administración y mantenimiento del sistema de red, sin tener que recurrir a equipos sofisticados o ayuda externa. Además minimiza la posibilidad de alteración de cableado.

Hasta ahora todo lo dicho se puede traducir en un ahorro de costos, lo cual es uno de los puntos más delicados en toda instalación de red ya que generalmente los costos son elevados. Muchas personas tienden a no poner un sistema de cableado estructurado para ahorrar en la inversión, sin embargo, del monto total necesario sólo el 2% corresponde a la instalación de dicho sistema; en contraste, el 50% de las fallas de una red son ocasionadas por problemas en la administración física, específicamente el cableado.

A pesar que el monto inicial de un cableado que no cumple con normas es menor que el de un cableado estructurado, este último significa un solo gasto en casi todo su tiempo de vida útil ya que ha sido planificado de acuerdo a las necesidades presentes y futuras de la red, lo cual implica modificaciones mínimas del diseño original en el futuro.

Además, se debe mencionar que todo cambio o modificación de una red se traduce en tiempos fuera de servicio mientras se realizan, lo cuales en muchas empresas significan menos productividad y puntos críticos si estos son muy prolongados. Por lo tanto un sistema de cableado estructurado, minimizará estos tiempos muertos.

En un sistema de cableado estructurado, se utiliza la topología tipo estrella, es decir que cada estación de trabajo se conecta a un punto central con un cable independiente al de otra estación. Esta concentración hará que se disponga de un conmutador o switch que sirva como bus activo y repetidor.

La ventaja de la concentración reside en la facilidad de interconexión, administración y mantenimiento de cada uno de los diferentes elementos. Además permite la comunicación con virtualmente cualquier dispositivo en cualquier lugar y en cualquier momento.

## 4.6. Estándar de Cableado para Telecomunicaciones en Edificios Comerciales: Norma ANSI/TIA/EIA 568-B

Fue creado para:

- Establecer especificaciones de cableado que soporten las aplicaciones de diferentes vendedores.
- Brindar una guía para el diseño de equipos de telecomunicaciones y productos de cableado para sistemas de telecomunicaciones de organizaciones comerciales.
- Especificar un sistema general de cableado suficiente para soportar aplicaciones de datos y voz.
- Proveer pautas para la planificación e instalación de sistemas de cableado estructurado.

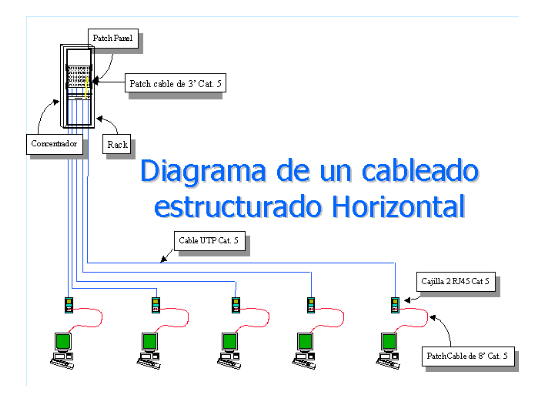
## 4.7. Subsistemas de Cableado Estructurado

La norma ANSI/TIA/EIA 568-B divide el cableado estructurado en siete subsistemas, donde cada uno de ellos tiene una variedad de cables y productos diseñados para proporcionar una solución adecuada para cada caso. Los distintos elementos que lo componen son los siguientes:

- Subsistema de cableado Horizontal
- Área de Trabajo
- Subsistema de cableado Vertical
- Cuarto de Telecomunicaciones
- Cuarto de Equipos
- Cuarto de Entrada de Servicio
- Subsistema de Administración

## 4.8. Subsistema de Cableado Horizontal

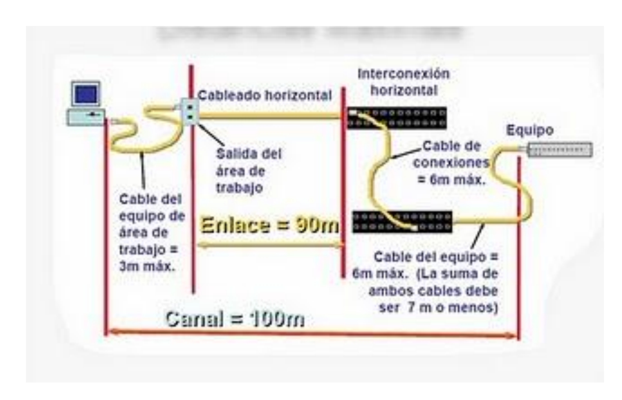
El cableado horizontal incorpora el sistema de cableado que se extiende desde el área de trabajo de telecomunicaciones hasta el cuarto de telecomunicaciones.




**Subsistema de Cableado Horizontal**

Está compuesto por:

- Cables horizontales: Es el medio de transmisión que lleva la información de cada usuario hasta los correspondientes equipos de telecomunicaciones. Según la norma ANSI/TIA/EIA-568-A, el cable que se puede utilizar es el UTP de 4 Pares (100 22/24 AWG), STP de 2 pares (150 22 AWG) y Fibra Óptica multimodo de dos hilos 62,5/150. Debe tener un máximo de 90 m. independiente del cable utilizado, sin embargo se deja un margen de 10 m. que consisten en el cableado dentro del área de trabajo y el cableado dentro del cuarto de telecomunicaciones (patchcord).




**Distancia Máxima Cableado Horizontal**

- Terminaciones Mecánicas: Conocidos como regletas o paneles (patchpanels); son dispositivos de interconexión a través de los cuales los tendidos de cableado horizontal se pueden conectar con otros dispositivos de red como, por ejemplo, switches. Es un arreglo de conectores RJ-45 que se utiliza para realizar conexiones cruzadas entre los equipos activos y el cableado horizontal. Se consiguen en presentaciones de 12, 24, 48 y 96 puertos.



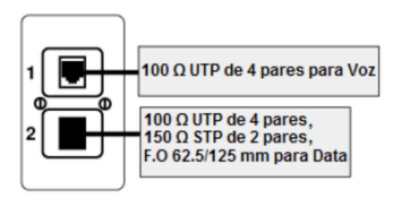
**Patch Panel y módulo Jack**

- Cables puentes: Conocidos como patchcords; son los cables que conectan diferentes equipos en el cuarto de telecomunicaciones. Estos tienen conectores a cada extremo, el cual dependerá del uso que se le quiera dar, sin embargo generalmente tienen un conector RJ-45. Su longitud es variable, pero no debe ser talque sumado a la del cable horizontal y la del cable del área de trabajo, resulte mayor a 100 m.



**PatchCord**

- Puntos de acceso: Conocidos como salida de telecomunicaciones u Outlets; Deben proveer por lo menos dos puertos uno para el servicio de voz y otro para el servicio de datos.




**Outlet**

- Puntos de Transición: También llamados puntos de consolidación; son puntos en donde un tipo de cable se conecta con otro tipo, por ejemplo cuando el cableado horizontal se conecta con cables especiales para debajo de las alfombras. Existen dos tipos:
    - Toma multiusuario: Es un outlet con varios puntos de acceso, es decir un outlet para varios usuarios.
    - CP: Es una conexión intermedia del cableado horizontal con un pequeño cableado que traen muchos muebles modulares.

  La norma permite sólo un punto de transición en el subsistema de cableado horizontal.

## 4.9. Área de trabajo

El área de trabajo es el espacio físico donde el usuario toma contacto con los diferentes equipos como pueden ser teléfonos, impresoras, FAX, PC’s, entre otros.

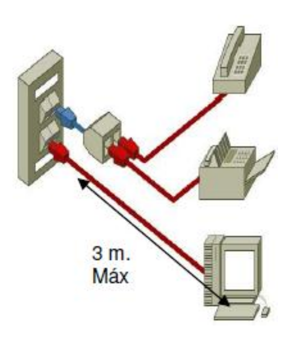
Se extiende desde el outlet hasta el equipo de la estación.

El cableado en este subsistema no es permanente y por ello es diseñado para ser relativamente simple de interconectar de tal manera que pueda ser removido, cambiado de lugar, o colocar uno nuevo muy fácilmente. Por esta razón es que el cableado no debe ser mayor a los 3 m.

Como consideración de diseño se debe ubicar un área de trabajo cada 10 m$^2$ y esta debe por lo menos de tener dos salidas de servicio, en otras palabras dos conectores. Uno de los conectores debe ser del tipo RJ-45 bajo el código de colores de cableadoT568A (recomendado) o T568B. Además, los ductos a las salidas del área de trabajo deben

prever la capacidad de manejar tres cables (Data, Voz y respaldo o Backus).

Cualquier elemento adicional que un equipo requiera a la salida del área de trabajo, no debe instalarse como parte del cableado horizontal, sino como componente externo a la salida del área de trabajo. Esto garantiza la utilización del sistema de cableado estructurado para otros usos.




**Outlet con adaptador**

## 4.10. Subsistema de Cableado Vertical

El cableado vertical, también conocido como cableado backbone, es aquel que tiene el propósito de brindar interconexiones entre el cuarto de entrada de servicios, el cuarto de equipo y cuartos de telecomunicaciones.

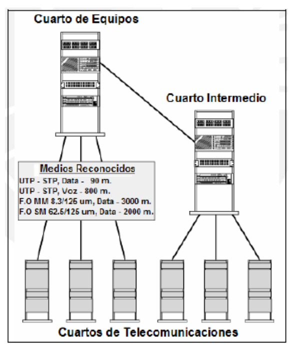
La interconexión se realiza con topología estrella ya que cada cuarto de telecomunicaciones se debe enlazar con el cuarto de equipos. Sin embargo se permite dos niveles de jerarquía ya que varios cuartos de telecomunicaciones pueden enlazarse a un cuarto de interconexión intermedia y luego éste se interconecta con el cuarto de equipo.

A continuación se detallan los medios que se reconocen para el cableado vertical y sus distancias:

| Medio | Aplicación | Distancia (metros) |
|---|---|---|
| 100 Ω UTP o STP | Data | 90 |
| 100 Ω UTP o STP | Voz | 800 |
| Fibra Monomodo 8,3/125 um. | Data | 3000 |
| Fibra Multimodo 62,5/125 um. | Data | 2000 |

Tipo de cableado reconocido y sus distancias máximas

Las distancias en esta tabla son las permitidas entre el cuarto de equipos y el cuarto de telecomunicaciones, permitiendo un cuarto intermedio.




Subsistema de Cableado Vertical

## 4.11. Cuarto de Telecomunicaciones

Es el lugar donde termina el cableado horizontal y se origina el cableado vertical, por lo que contienen componentes como patchpanels. Pueden tener también equipos activos de LAN como por ejemplo switches, sin embargo generalmente no son dispositivos muy complicados. Estos componentes son alojados en un bastidor, mayormente conocido como rack o gabinete, el cual es un armazón metálico que tiene un ancho estándar de 19’’ y tiene agujeros en sus columnas a intervalos regulares llamados unidades de rack (RU) para poder anclar el equipamiento. Dicho cuarto debe ser de uso exclusivo de equipos de telecomunicaciones y por lo menos debe haber uno por piso siempre y cuando no se excedan los 90 m. especificados para el cableado horizontal.

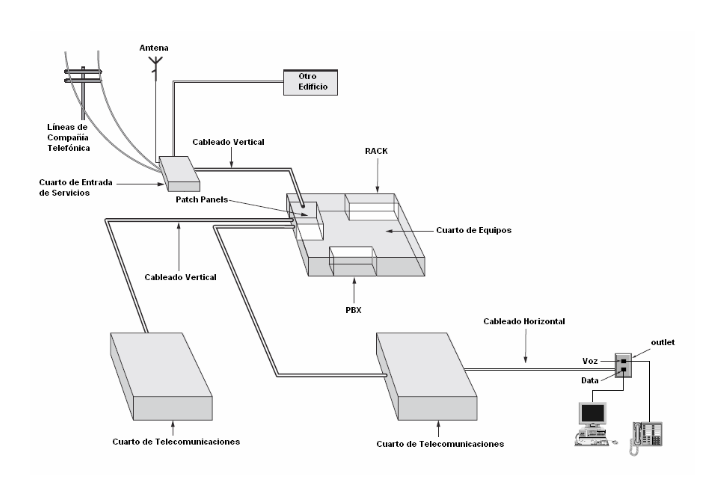
## 4.12. Cuarto de Equipos

El cuarto de equipos es el lugar donde se ubican los principales equipos de telecomunicaciones tales como centrales telefónicas, switches, routers y equipos de cómputo como servidores de datos video. Además éstos incluyen uno o varias áreas de trabajo para personal especial encargado de estos equipos. Se puede decir entonces que los cuartos de equipo se consideran distintos de los cuartos de telecomunicaciones por la naturaleza, costo, tamaño y complejidad del equipo que contienen.

## 4.13. Cuarto de Entrada de Servicios

Es el lugar donde se encuentra la acometida de los servicios de telecomunicaciones, por lo tanto es el punto en donde el cableado interno deja el edificio y sale hacia el exterior. Es llamado punto de demarcación pues en el "terminan" los servicios que brinda un proveedor, es decir que pasado este punto, el cliente es responsable de proveer los equipos y cableado necesario para dicho servicio, así como su mantenimiento y operación.

El cuarto de entrada también recibe el backbone que conecta al edificio a otros en situaciones de campus o sucursales.




**Interconexión del Cuarto de Equipos**

## 4.14. Estándar de Rutas y Espacios de Telecomunicaciones para Edificios Comerciales: Norma ANSI/TIA/EIA 569-A

El objetivo de esta norma es brindar una guía estandarizada para el diseño de sistemas de cableado estructurado, la cual incluye detalles acerca de las rutas de cables y espacios para equipos de telecomunicaciones en edificios comerciales. Hace referencia a los subsistemas definidos por la norma ANSI/TIA/EIA 568-B.

Los espacios de telecomunicaciones como el cuarto de equipos, los cuartos de telecomunicaciones o el cuarto de entrada de servicios tienen reglas de diseño en común:

- Las puertas (sin considerar el marco) deben abrirse hacia fuera del cuarto, deslizarse hacia un costado o ser removibles. Sus medidas mínimas son 0,91 m. de ancho por 2 metros de alto.
- La energía eléctrica debe ser suministrada por al menos 2 outletsque provengan de circuitos diferentes. Esto es aparte de las necesidades eléctricas que se requieran en el cuarto por los equipos que se tengan.
- La iluminación debe tener una intensidad de 500 lx y el switch debe estar localizado cerca de la entrada.
- Estos espacios no deben tener falsos techos.
- Cualquier pasante hecho en las paredes protegidas contraincendios deberán ser sellados para evitar la propagación.
- Cualquier ruta de cableado deberá evitar cualquier clase de interferencia electromagnética.
- Se debe cumplir con la norma ANSI/TIA/EIA 607

## 4.15. Cuarto de Entrada de Servicios

- Generalmente está ubicado en el sótano o el primer piso.
- Puede requerir una entrada alternativa
- Al menos una de las paredes debe ser de 20 mm. de A-Cplywood
- Debe ser un área seca, donde se puedan evitar inundaciones
- Se debe tratar que este lo más cerca posible de la ruta por donde entran los cables al edificio.
- No debe contener equipos que no estén relacionados con la entrada de los servicios

## 4.16. Cuarto de Equipos

- La temperatura en el cuarto debe ser controlada todo el tiempo, por lo que se debe utilizar sistemas de HVAC. Debe estar entre 18º a 24º con una humedad relativa de 30% a 55%. Se recomienda instalar un sistema de filtrado de aire que proteja a los equipos contra la contaminación como por ejemplo el polvo.
- Se deben tomar precauciones contra sismos o vibraciones.
- El techo debe estar por lo menos a 2,4 m.
- Se recomienda tener una puerta doble, ya que la entrada debe ser lo suficientemente amplia para que se puedan ingresar los equipos sin dificultad.
- El cuarto debe estar por encima del nivel del agua para evitar daños por inundaciones.
- El cuarto de equipos y el cuarto de entrada de servicios pueden ser el mismo.

## 4.17. Cuarto de Telecomunicaciones

- Debe haber uno por cada piso
- Se deben tener medidas de control de la temperatura.
- Idealmente estos cuartos deben estar alineados verticalmente lo largo de varios pisos para que el cableado vertical sea lomas recto posible.
- Dos paredes deben ser de 20 mm. de A-C plywood y éste debe ser de 2,4 m. de alto.
- Se deben tomar precauciones contra sismos.

## 4.18. Rutas del cableado horizontal

- Generalmente la ruta que recorre el cableado horizontal se encuentra entre el techo de la estructura y el falso techo.
- El cableado no puede estar apoyado sobre el falso techo.
- En el caso de tender el cable sin ningún tipo de estructura de sujeción, se deben usar elementos que sujeten el cable al techo como por ejemplo los ganchos “J”, estos sujetadores deben colocarse máximo cada 60‘’ (1,52 m.).
- En el caso de usarse bandejas o ductos (conduits), éstos pueden ser de metal o de plástico.

## 4.19. Requerimientos de puesta y conexiones a tierra para telecomunicaciones: Norma ANSI/TIA/EIA 607

El sistema de puesta a tierra es muy importante en el diseño de una red ya que ayuda a maximizar el tiempo de vida de los equipos, además de proteger la vida del personal a pesar de que se trate de un sistema que maneja voltajes bajos. Aproximadamente el 70% de anomalías y problemas asociados a sistemas distribución de potencia son directa o indirectamente relacionados a temas de conexiones y puestas a tierra [42]. A pesar de esto, el sistema de puesta a tierra es uno de los componentes del cableado estructurado más obviados en la instalación.

El estándar que describe el sistema de puesta a tierra para las redes de telecomunicaciones es ANSI/TIA/EIA-607. El propósito principal es crear un camino adecuado y con capacidad suficiente para dirigir las corrientes eléctricas y voltajes pasajeros hacia la tierra. Estas trayectorias a tierra son más cortas de menor impedancia que las del edificio.

A continuación se explicarán términos básico para entender un sistema de puesta a tierra en general:

- Puesta a tierra (grounding): Es la conexión entre un equipo o circuito eléctrico y la tierra
- Conexión equipotencial a tierra (bonding): Es la conexión permanente de partes metálicas para formar una trayectoria conductora eléctrica que asegura la continuidad eléctrica y la capacidad de conducir de manera segura cualquier corriente que le sea impuesta.
- Conductor de enlace equipotencial para telecomunicaciones (BCT): Es un conductor de cobre aislado que interconecta el sistema de puesta a tierra de telecomunicaciones al sistema de puesta a tierra del edificio. Por lo tanto une el TMGB con la puesta a tierra del sistema de alimentación. Debe ser dimensionado al menos de la misma sección que el conductor principal de enlace de telecomunicaciones (TBB). No debe llevarse en conductos metálicos.
- Barra de tierra principal de telecomunicaciones (TMGB): Es una barra que sirve como una extensión dedicada del sistema de electrodos de tierra (pozo a tierra) del edificio para la infraestructura de telecomunicaciones. Todas las puestas a tierra de telecomunicaciones se originan en él, es decir que sirve como

conexión central de todos los TBB's del edificio. Consideraciones del diseño:

- Usualmente se instala una por edificio.
- Generalmente está ubicada en el cuarto de entrada de servicios
- en el cuarto de equipos, en cualquiera de los casos se tiene que tratar de que el BCT sea lo más cortó y recto posible.
- Montada en la parte superior del tablero o caja.
- Aislada del soporte mediante aisladores poliméricos (50 mm.mínimo)
- Hecha de cobre y sus dimensiones mínimas 6 mm. de espesor y100 mm. de ancho. Su longitud puede variar, de acuerdo a la cantidad de cables que deban conectarse a ella y de las futuras conexiones que tendrá**.**

▪ Barra de tierra para telecomunicaciones (TGB): Es la barra de tierra ubicada en el cuarto de telecomunicaciones o de equipos que sirve de punto central de conexión de tierra de los equipos de la sala. Consideraciones del diseño:
  - Cada equipo o gabinete ubicado en dicha sala debe tener suTGB montada en la parte superior trasera.
  - El conductor que une el TGB con el TBB debe ser cable 6 AWG. Además se debe procurar que este tramo sea lo más recto y corto posible.
  - Hecha de cobre y sus dimensiones mínimas 6 mm. de espesor y50 mm. de ancho. Su longitud puede variar, de acuerdo a la cantidad de cables que deban conectarse a ella y de las futuras conexiones que tendrá.
  - Aislada mediante aisladores poliméricos (h=50 mm mínimo)

▪ Conductor central de enlace equipotencial de Telecomunicaciones (TBB): Es un conductor aislado de cobre utilizado para conectar todos los TGB's al TMGB. Su principal función es la de reducir o ecualizar todas las diferencias de potencial de todos los sistemas de telecomunicaciones enlazados a él. Consideraciones del diseño:
  - Se extiende a través del edificio utilizando la ruta del cableado vertical.
  - Se permite varios TBB's dependiendo del tamaño del edificio.

- Cuando dos o más TBB's se usen en un edificio de varios pisos, éstos deberán ser unidos a través de un TBBIBC en el último piso y cada tres pisos.
- Su calibre debe ser mínimo 6 AWG y máximo 3/0 AWG, por lo tanto se deberá usar un conductor de cobre aislado cuya sección acepte estas medidas.
- El estándar ha establecido una tabla para diseñar este conductor de acuerdo a su distancia:

| Longitud del TBB (m) | Calibre (AWG) |
|---|---|
| Menor a 4 | 6 |
| 4 - 6 | 4 |
| 6 – 8 | 3 |
| 8 – 10 | 2 |
| 10 – 13 | 1 |
| 13 – 16 | 1/0 |
| 16 – 20 | 2/0 |
| Mayor a 20 | 3/0 |

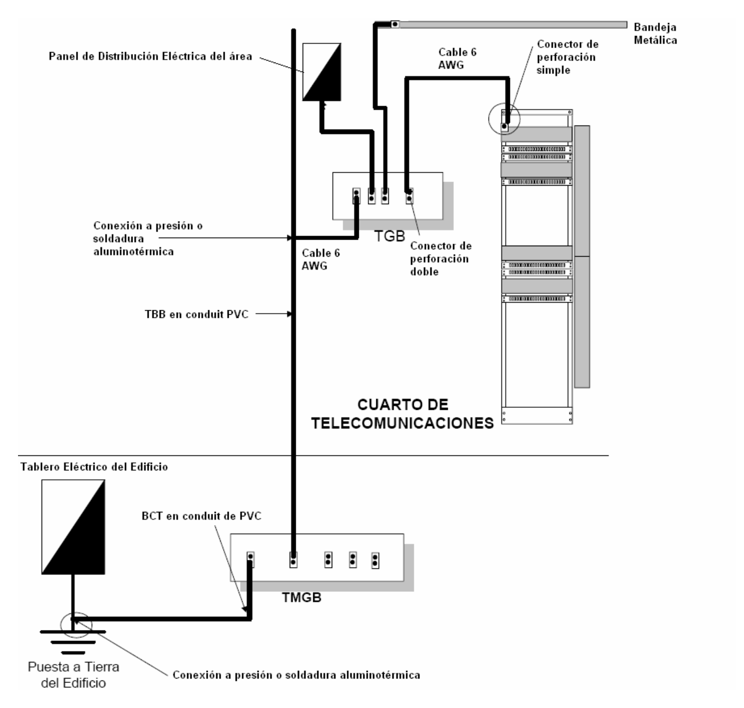
**Dimensionamiento del TBB**

- Deben evitarse empalmes, pero sí de todas maneras existen estos deben estar ubicados en algún espacio de telecomunicaciones.

Es importante mencionar que los conectores usados en la TMGB y los usados en la conexión entre el TBB y el TGB, deberán ser descompresión de dos perforaciones. Mientras que la conexión de conductores para unir equipos de telecomunicaciones a la TMGB o TGB pueden ser conectores de compresión por tornillo de una perforación, aunque no es lo más recomendable debido a que pueden aflojarse por cualquier movimiento.

Todos los elementos metálicos que no lleven corriente en el sistema de cableado estructurado deberán ser aterrados, como por ejemplo bastidores (racks), bandejas o conduits.

Por último, cualquier doblez que se tenga que realizar a los cables no debe ser mayor a 2,54 cm.




**Puesta a Tierra para Telecomunicaciones**

## 4.20. Medios de Transmisión

Una de los puntos más importante es definir el tipo de medio de transmisión que se va a utilizar. Se describirán los medios reconocidos por la norma ANSI/TIA/EIA 568-B ya que es el estándar que se seguirá en el presente trabajo.

## 4.21. Cable UTP (Unshield Twisted Pair)

Está formado por alambres de cobre entrelazados para disminuir efectos de interferencia electromagnética (EMI) de fuentes externas. Se dice que no es apantallado porque ambos conductores están aislados con una cubierta de PVC.

Existen diferentes categorías las cuales en común tienen el uso de 4 pares de conductores y presentar varios tipos de diafonía (ocrosstalk, señales acopladas de un par a otro). Se diferencian entre sí por tener diferentes valores en parámetros de transmisión, muchos de los cuales

hacen referencia al nivel de diafonía que presenta el cable. Los parámetros de transmisión más referenciados son:

- Atenuación en función de la frecuencia (db): Se define como la pérdida de fuerza de una señal al atravesar toda la longitud del cable. Es causada por pérdidas de energía eléctrica debido a la resistencia del cable y por fugas de energía a través del aislamiento del mismo. Las pérdidas por resistencia del cable se incrementan si la frecuencia de la señal aumenta y las fugas a través del aislamiento se incrementan con el aumento de la temperatura. Cuanto más bajo sea este valor, se obtienen mejores resultados.
- Pérdidas de Inserción (dB): Es la pérdida de la potencia de la señal transmitida debido a la inserción del cable entre la fuente (Tx) y la carga (Rx). Su valor es la relación entre la potencia recibida y la potencia transmitida, por ello lo ideal es que dicho valor sea lo más cercano a 0dB.
- NEXT (db): Medida del acoplamiento de la señal entre un par y otro. Lo produce una señal inducida que vuelve y es percibida en el lado del emisor. Varía proporcionalmente con la frecuencia, cuanto más alto es el valor es mejor.
- PSNEXT (dB): El Power Sum NEXT se define como el efecto acumulativo de los efectos NEXT individuales en cada par debido a los otros tres.
- FEXT (dB): Es también una medida del acoplamiento de señal entre un par y otro, solo que lo produce una señal inducida que es percibida en el lado del receptor. Es más débil que el NEXT.
- ELFEXT (dB): Se expresa en dB como la diferencia entre la medida FEXT y la pérdida de inserción. Cuanto más alto es el valor es mejor.
- PSELFEXT (dB): El Power Sum ELFEXT se define como el efecto acumulativo de los efectos ELFEXT individuales en cada par debido a los otros tres.
- Pérdida de Retorno (dB): La pérdida de retorno expresa qué cantidad de potencia de la señal incidente (al receptor) se refleja. Puede causar interferencias con la señal transmitida o daños en el equipo transmisor. A mayor valor es mejor.
- Rango de Frecuencias: Ancho de banda en donde los valores de los demás parámetros de transmisión son efectivos, por lo que se dice que en determinado rango de frecuencias se transmitirá una señal adecuada. A mayor frecuencia de la portadora se obtiene

un mayor ancho de banda y a mayo rancho de banda, mayor velocidad de transmisión de datos.

En la siguiente tabla se muestran las categorías de cable UTP actualmente reconocidas por los estándares con sus características más resaltantes:

| | CATEGORÍA | |
|---|---|---|
| | 5e @155 Mhz | 6 @155 Mhz |
| Rango de Frecuencias (MHz) | 1 – 155 | 1 – 250 |
| Atenuación (dB) | 29,1 | 20,2 |
| NEXT (dB) | 29,8 | 45,9 |
| ELFEXT (dB) | 18 | 29,3 |
| Pérdida de Retorno (dB) | 9,1 | 16 |

**Comparación de parámetros de transmisión entre cables UTP cat. 5e y 6**

| | CATEGORÍA | | |
|---|---|---|---|
| | 6 @250 Mhz | 6A @250 Mhz | 6A @500 MHz |
| Rango de Frecuencias (MHz) | 1 – 250 | 1 – 500 | 1 – 500 |
| Atenuación (dB) | 34,1 | 32,9 | 47,8 |
| NEXT (dB) | 39,1 | 39,1 | 28,9 |
| ELFEXT (dB) | 21,3 | 35 | 29 |
| Pérdida de Retorno (dB) | 12 | 11 | 6 |

**Comparación de parámetros de transmisión entre cables UTP de cat. 6 y 6A**

## 4.22. Fibra Óptica

Es un conductor no metálico conformado por filamentos de vidrio. Su forma de transmitir señales es mediante la transmisión de luz a través del principio de reflexión interna total. Por lo tanto no sufre de efectos EMI ni diafonía, lo que ayuda a alcanzar grandes distancias. Gracias a que se trabaja con frecuencias ópticas, se obtienen anchos de banda muy grandes. Existen dos tipos:

Multimodo: Se transmiten varios modos de luz (trayectorias) que se logra teniendo un núcleo de tamaño típico de 50 ó 62,5 um.

Debido a que existe dispersión por los diferentes modos propagados se alcanzan distancias promedio de 1 a 2 Km.

Monomodo: Se transmite solo un modo de luz que se logra reduciendo el diámetro del núcleo generalmente de 9 um. Gracias que no hay dispersión por causa de varias trayectorias, se alcanzan distancias mayores, hasta de 100 Km. Algunos parámetros a considerar al escoger un sistema de fibra óptica son:

- Ventana de Transmisión: Rango de longitud de onda donde se puede transmitir y detectar luz con máxima eficiencia. Es decirla longitud de onda en la cual trabajará el sistema.
- Atenuación: Cada ventana tiene un determinado coeficiente de atenuación; a mayor ventana, menor atenuación. Por otro lado, dependerá directamente de la longitud por lo que se expresa en dB/Km. (A=_/L)
- Ángulo de Aceptación: Máximo ángulo con el cual debe incidirla luz en la fibra para lograr el efecto de reflexión interna total.
- Apertura Numérica: Es un indicado que da idea de la cantidad de luz que puede ser guiada. Por lo tanto cuanto mayor es, mayor es la cantidad de luz que puede aceptar en su núcleo.
- Dispersión Intermodal: resulta de la diferencia en el tiempo de propagación entre los modos que siguen trayectorias diferentes (ensanchamiento del pulso). Limita el ancho de banda.
- Dispersión Intermodal: Resulta de la diferencia en el tiempo de propagación de las diferentes componentes espectrales de la señal transmitida. Limita el ancho de banda.

## 4.23. Administración para Infraestructura de Telecomunicaciones de Edificios Comerciales: Norma TIA/EIA 606.

La manera de cómo rotular todos los componentes de un sistema de cableado estructurado está definido en la norma TIA/EIA 606, el cual provee un esquema de administración uniforme, es decir que rige para todos los aspectos del cableado estructurado. Además esta forma de identificar los diferentes elementos es independiente de las aplicaciones que se le dé al cableado, ya que muchas veces las aplicaciones van variando a lo largo de los años.

El sistema de administración simplifica traslados, agregados, cambios permitiendo que los trabajos que se realicen requieran pocas

suposiciones. Además, facilita los trabajos de mantenimiento ya que los componentes con posibles fallas son fácilmente identificados durante las labores de reparación.

Las etiquetas deben ser de un tamaño, color y contraste apropiado para asegurar su lectura y deben procurar tener un tiempo de vida igualo mayor a la del componente etiquetado. Para mayor confiabilidad se sugiere que las etiquetas sean hechas por algún dispositivo y no a mano.

Los componentes a ser etiquetados son:

- Espacios de Telecomunicaciones
- Cables
- Hardware
- Puestas a Tierra

Se establecen cuatro clases de administración dependiendo del tamaño de la red y por lo tanto del tipo de componentes de cableado estructurado que lo integran.

Clase 1

Dirigida a infraestructuras que poseen solo un cuarto de equipos, por lo tanto será el único espacio de telecomunicaciones a administrar. No tendrá cableado vertical o externo a la planta. Se identificarán los siguientes elementos:

- Espacio de Telecomunicaciones
- Cableado horizontal
- TMGB
- TGB

Clase 2

Provee administración para un único edificio que tiene uno o múltiples espacios de telecomunicaciones como por ejemplo un cuarto de equipos y uno o más cuarto de telecomunicaciones. Incluye, aparte de todos los elementos de la clase 1, administración para el cableado vertical, puntos de seguridad contra incendios y múltiples elementos del sistema a puesta a tierra.

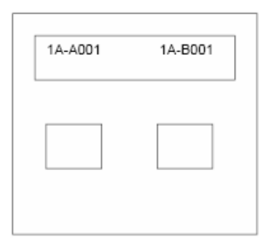
Clase 3

Dirigida a edificios dentro de un campus, es decir que cubre la identificación de elementos tanto dentro como fuera del edificio. Inclúyelas identificaciones de las clases anteriores e identificación de

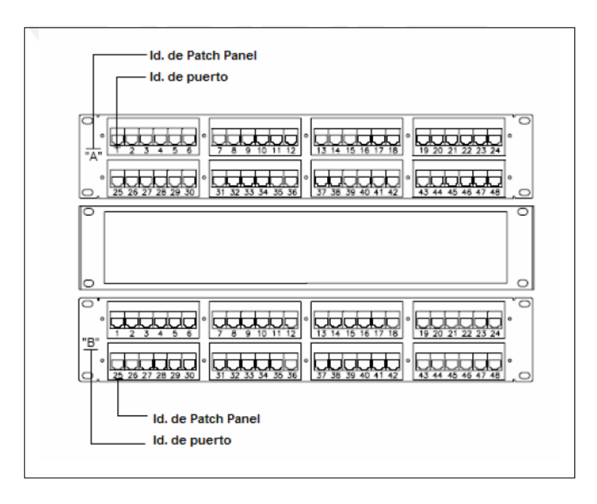
edificio dentro del campus y cableado de backbone de interconexión entre edificios.

Clase 4

Dirigido a los sistemas de cableado estructurado que abarcan varios campus, es decir un ambiente multi-campus. Incluye identificación de las clases anteriores y del lugar al que corresponden.




**Outlet con faceplate etiquetado**




**Patch Panels etiquetados**

La norma TIA/EIA-606 establece que de manera opcional se pueden identificar los elementos del camino de los diferentes cableados, como por ejemplo tuberías, conductos, bandejas o canaletas.

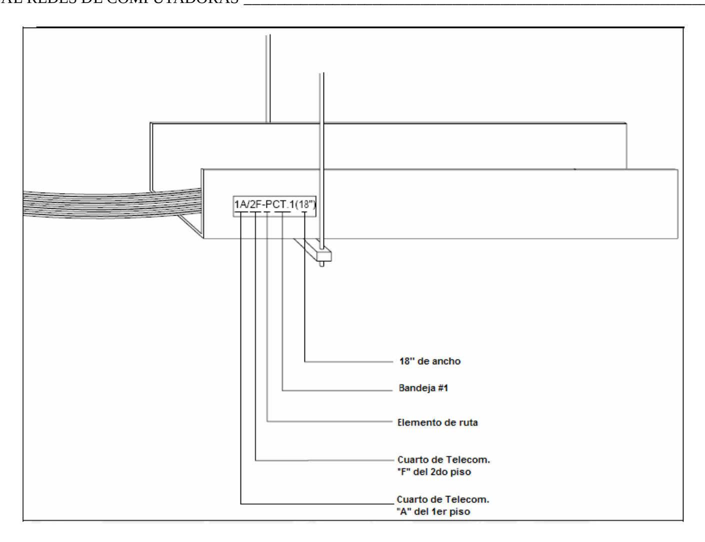



**Figura 2.12 – Bandeja etiquetada**

## *Preguntas propuestas*

1.- ¿Cómo se representa una señal de datos?

2.- ¿en un medio de transmisión se pierde la señal?

3.- ¿Qué es la razón de BAUD?

4.- ¿Qué determina el ancho de banda de un canal?

5.- Si tenemos un canal de ancho de banda H (en Hertz) y V niveles discretos de señal ¿Cuáles la velocidad máxima en un canal perfecto (en bits por segundo)?

6.- ¿Cómo se expresa un dB?

7.- ¿cuál es la velocidad máxima en bps de un canal con ancho de banda H Hz y razón de señal a ruido de S/R?

8.- Si una línea telefónica tiene un S/R de 30 dB (o 1000) ¿Cuál es la velocidad máxima en bps, que puede transmitir?

***Respuestas a las preguntas propuestas***

1.-

- Se puede representar cualquiera señal de datos con una serie Fourier.
- La serie consiste en términos de frecuencias distintas y se suman los términos para reconstruir la señal.

2.-

- Ningún medio de transmisión puede transmitir señales sin perder algún poder.
- Normalmente un medio puede transmitir las frecuencias desde 0 hasta algún límite f; las frecuencias mayores se atenúan fuertemente.

3.-

- Cuanto más cambios por segundo de una señal (la razón de baud), tanto más términos de frecuencias altas que se necesitan.

4.-

- El ancho de banda de un canal determina la velocidad de la transmisión de datos, aun cuando el canal es perfecto.

5.-

$$vmax = 2H \log2V$$

Esto es el teorema de Nyquist.

6.-

- Si el poder de la señal es S y el poder de ruido es R, la razón de señal a ruido es S/R.
- Normalmente se expresa esta razón en los decibeles (dB), que son:

$$dB = 10\log_{10}(S/R)$$

7.-

$$vmax = H \log_2(1+S/R)$$

Es debido a Shannon.

8.-

- no puede transmitir más de 30.000 bps, independientemente del número de niveles de señal.

Capítulo 5

# *CAPA ENLACE DE DATOS*

## 5.1. Protocolos

En cada una de las capas de los modelos que estudiamos (excepto en la capa física) se utiliza un protocolo distinto. Estos protocolos se van apilando de forma que los de capas superiores aprovechan los servicios de los protocolos de capas inferiores. Durante una transmisión cada protocolo se comunica con su homónimo del otro extremo sin preocuparse de los protocolos de otras capas.

Una de las decisiones más importantes que debemos tomar a la hora de diseñar una red es elegir un protocolo de la capa de acceso al medio y otro de las capas de red y transporte. A continuación estudiamos los distintos protocolos. Adelantamos, no obstante, que la combinación más interesante para redes locales nuevas es Ethernet + TCP/IP.

## 5.2. Protocolos de la capa de acceso al medio

En la capa de acceso al medio se determina la forma en que los puestos de la red envían y reciben datos sobre el medio físico. Se responden preguntas del tipo: ¿puede un puesto dejar información en el cable siempre que tenga algo que transmitir?, ¿debe esperar algún turno?, ¿cómo sabe un puesto que un mensaje es para él?

Un organismo de normalización conocido como IEEE (Instituto de ingenieros eléctricos y electrónicos) ha definido los principales protocolos de la capa de acceso al medio conocido en conjunto como estándares 802. Los más importantes son los IEEE 802.3 y IEEE 802.5 que se estudian a continuación.

***Otros estándares 802.--*** *El estándar 802.1 es una introducción al conjunto de estándares y define algunos aspectos comunes. El estándar 802.2 describe la parte superior de la capa de enlace de datos del modelo OSI (entre la capa de acceso al medio y la capa de red) que puede proporcionar control de errores y control de flujo al resto de estándares 802 utilizando el protocolo LLC (Logical Link*

*Control, control lógico de enlace). Las normas 802.3 a 802.5 definen protocolos para redes LAN. El estándar 802.4 que no vamos a estudiar por su escasa implantación se conoce como Token Bus (bus con paso de testigo). Finalmente, 802.6 es un estándar adecuado para utilizarse en redes MAN. Se trata de DQDB (Distributed Queue Dual Bus, bus doble de colas distribuidas).*

El protocolo utilizado en esta capa viene determinado por las tarjetas de red que instalemos en los puestos. Esto quiere decir que si adquirimos tarjetas Ethernet sólo podremos instalar redes Ethernet. Y que para instalar redes Token ring necesitaremos tarjetas de red especiales para Token ring. Actualmente en el mercado únicamente se comercializan tarjetas de red Ethernet (de distintas velocidades y para distintos cableados).

### *Token ring (802.5)*

Las redes Token ring (paso de testigo en anillo) fueron utilizadas ampliamente en entornos IBM desde su lanzamiento en el año 1985. En la actualidad es difícil encontrarlas salvo en instalaciones antiguas de grandes empresas.

El cableado se establece según una topología de anillo. En lugar de utilizar difusiones, se utilizan enlaces punto a punto entre cada puesto y el siguiente del anillo. Por el anillo Token ring circula un mensaje conocido como *token* o ficha. Cuando una estación desea transmitir espera a recibir el token. En ese momento, lo retira de circulación y envía su mensaje. Este mensaje circula por el anillo hasta que lo recibe íntegramente el destinatario. Entonces se genera un token nuevo.

Las redes Token ring utilizan una estación monitor para supervisar el funcionamiento del anillo. Se trata de un protocolo complejo que debe monitorizar en todo momento el buen funcionamiento del token (que exista exactamente uno cuando no se transmiten datos) y sacar del anillo las tramas defectuosas que no tengan destinatario, entre otras funciones.

Las redes Token ring de IBM pueden funcionar a 4 Mbps o a 16 Mbps utilizando cable par trenzado o cable coaxial.

### *Ethernet (802.3)*

Las redes Ethernet son actualmente las únicas que tienen interés para entornos LAN. El estándar 802.3 fue diseñado originalmente para

funcionar a 10 Mbps, aunque posteriormente ha sido perfeccionado para trabajar a 100 Mbps (802.3u) o 1 Gbps.

Una red Ethernet tiene las siguientes características:

- *Canal único.* Todas las estaciones comparten el mismo canal de comunicación por lo que sólo una puede utilizarlo en cada momento.
- Es de *difusión* debido a que todas las transmisiones llegan a todas las estaciones (aunque sólo su destinatario aceptará el mensaje, el resto lo descartarán).
- Tiene un *control de acceso distribuido* porque no existe una autoridad central que garantice los accesos. Es decir, no hay ninguna estación que supervise y asigne los turnos al resto de estaciones. Todas las estaciones tienen la misma prioridad para transmitir.

## 5.3. Comparación de Ethernet y Token ring

*En Ethernet cualquier estación puede transmitir siempre que el cable se encuentre libre; en Token ring cada estación tiene que esperar su turno. Ethernet utiliza un canal único de difusión; Token ring utiliza enlaces punto a punto entre cada estación y la siguiente. Token ring tiene siempre una estación monitor que supervisa el buen funcionamiento de la red; en Ethernet ninguna estación tiene mayor autoridad que otra. Según esta comparación, la conclusión más evidente es que, a iguales velocidades de transmisión, Token ring se comportará mejor en entornos de alta carga y Ethernet, en redes con poco tráfico.*

En las redes Ethernet, cuando una estación envía un mensaje a otra, no recibe ninguna confirmación de que la estación destino haya recibido su mensaje. Una estación puede estar enviando paquetes Ethernet a otra que está desconectada y no advertirá que los paquetes se están perdiendo. Las capas superiores (y más concretamente, TCP) son las encargadas de asegurarse que la transmisión se ha realizado de forma correcta.

El protocolo de comunicación que utilizan estas redes es el CSMA/CD (*Carrier Sense Multiple Access / Collision Detect*, acceso múltiple con detección de portadora y detección de colisiones). Esta técnica de control de acceso a la red ha sido normalizada constituyendo el estándar IEEE 802.3. Veamos brevemente el funcionamiento de CSMA/CD.

Cuando una estación quiere transmitir, primero escucha el canal (detección de portadora). Si está libre, transmite; pero si está ocupado, espera un tiempo y vuelve a intentarlo.

Sin embargo, una vez que una estación ha decidido comenzar la transmisión puede darse el caso de que otra estación haya tomado la misma decisión, basándose en que el canal estaba libre cuando ambas lo comprobaron. Debido a los retardos de propagación en el cable, ambas señales colisionarán y no se podrá completar la transmisión de ninguna de las dos estaciones. Las estaciones que están transmitiendo lo advertirán (detección de colisiones) e interrumpirán inmediatamente la transmisión. Después esperarán un tiempo aleatorio y volverán a intentarlo. Si se produce una nueva colisión, esperarán el doble del tiempo anterior y lo intentarán de nuevo. De esta manera, se va reduciendo la probabilidad de nuevas colisiones.

Debemos recordar que el canal es único y por lo tanto todas las estaciones tienen que compartirlo. Sólo puede estar una estación transmitiendo en cada momento, sin embargo pueden estar recibiendo el mensaje más de una.

***Nota:*** *La existencia de colisiones en una red no indica que exista un mal funcionamiento. Las colisiones están definidas dentro del protocolo Ethernet y no deben ser consideradas como una situación anómala. Sin embargo, cuando se produce una colisión el canal se desaprovecha porque ninguna estación logra transmitir en ese momento. Debemos tratar de reducir el número de colisiones que se producen en una red. Esto se consigue separando grupos de computadores mediante un* switch *o un router. Podemos averiguar las colisiones que se producen en una red observando el correspondiente LED de nuestro* hub.

## 5.4. Direcciones físicas

¿Cómo sabe una estación que un mensaje es para ella? Está claro, que hay que distinguir unas estaciones de otras utilizando algún identificador. Esto es lo que se conoce como *direcciones físicas*.

Los adaptadores Ethernet tienen asignada una dirección de 48 bits de fábrica que no se puede variar. Los fabricantes nos garantizan que no puede haber dos tarjetas de red con la misma dirección física. Si esto

llegase a ocurrir dentro de una misma red la comunicación se volvería imposible. Los tres primeros bytes corresponden al fabricante (no puede haber dos fabricantes con el mismo identificador) y los tres últimos al número de serie (no puede haber dos tarjetas del mismo fabricante con el mismo número de serie). Por ejemplo,

5D:1E:23:10:9F:A3

Los bytes 5D:1E:23 identifican al fabricante y los bytes 10:9F:A3 al número de serie del fabricante 5D:1E:23

***Nota:*** *Los comandos* **ipconfig / all |more** *y* **winipcfg** *muestran la dirección física de nuestra tarjeta de red Ethernet. Observe que estos comandos pueden recoger también información relativa al adaptador virtual "PPP Adapter" (se corresponde con el módem o adaptador RDSI) además de la referente a la tarjeta de red real.*

No todas las direcciones representan a máquinas aisladas, algunas de ellas se utilizan para enviar mensajes de multidifusión. Esto es, enviar un mensaje a varias máquinas a la vez o a todas las máquinas de la red. Ethernet permite que el mismo mensaje pueda ser escuchado por más de una máquina a la vez.

## 5.5. Formato de la trama

La comunicación entre una estación y otra a través de una red Ethernet se realiza enviando tramas Ethernet. El mensaje que se quiere transmitir se descompone en una o más tramas con el siguiente formato:

**Tabla 9**

| **8 bytes** | **6 bytes** | **6 bytes** | **2 bytes** | **64-1500 bytes** | **4 bytes** |
|---|---|---|---|---|---|
| **Preámbulo** | Dirección física destino | Dirección física origen | Tipo de trama | Datos de la trama | CRC |

Las *direcciones origen* y *destino* son las direcciones físicas de los adaptadores de red de cada computador. El campo *Tipo de trama* indica el formato de los datos que se transfieren en el campo *Datos de la trama*. Por ejemplo, para un datagrama IP se utiliza el valor hexadecimal de 0800 y para un mensaje ARP el valor 0806. Todos los mensajes (*datagramas*) que se envíen en la capa siguiente irán

encapsulados en una o más tramas Ethernet utilizando el campo *Datos de la trama*. Y esto mismo es aplicable para cualquier otro tipo de red distinta a Ethernet. Como norma general, cada mensaje que transmite una capa se coloca en el campo datos de la capa anterior. Aunque es muy frecuente que el mensaje no quepa en una sola trama y se utilicen varias.

## 5.6. Velocidades

Ethernet puede funcionar a tres velocidades: 10 Mbps, 100 Mbps (*FastEthernet*) y 1 Gbps (1000 Mbps).

10 Mbps es la velocidad para la que se diseñó originalmente el estándar Ethernet. Sin embargo, esta velocidad se ha mejorado para adaptarse a las crecientes exigencias de las redes locales. La velocidad de 100 Mbps es actualmente la más utilizada en la empresa. Las redes a 1 Gbps están comenzado a ver la luz en estos momentos por lo que tardarán un tiempo en implantarse en el mercado (los precios son todavía muy altos).

Para crear una red que trabaje a 10 Mbps es suficiente con utilizar cable coaxial o bien, cable par trenzado de categoría 3 o superior. Sin embargo, es recomendable utilizar cables par trenzado de categoría 5 y concentradores con velocidades mixtas 10/100 Mbps. De esta forma, en un futuro se podrán ir cambiando gradualmente los adaptadores de 10 Mbps por unos de 100 Mbps sin necesidad de instalar nuevo cableado.

La mejor opción actualmente para redes nuevas es *FastEthernet*. Para conseguir velocidades de 100 Mbps es necesario utilizar cable par trenzado con una categoría mínima de 5, un concentrador que soporte esta velocidad y tarjetas de red de 100 Mbps. Generalmente, los cables UTP cumplen bien con su función pero en situaciones concretas que requieran el máximo rendimiento de la red o existan muchas interferencias, puede ser necesario un cableado STP.

## 5.7. Tipos de adaptadores

La siguiente tabla resume los principales tipos de adaptadores Ethernet en función del cableado y la velocidad de la red. (T se utiliza para par trenzado, F para fibra óptica y X para *FastEthernet*).

**Tabla 10**

| | 10Base5 | 10Base2 | 10BaseT | 10BaseFP | 100BaseTX | 100BaseFX |
|---|---|---|---|---|---|---|
| Cableado | Coaxial | | Par trenzado | Par de fibra óptica | Par trenzado | 2 fibras ópticas |
| Velocidad | 10 Mbps | | | | 100 Mbps | |
| Topología | Bus | | Estrella | | | |
| Longitud máxima segmento | 500 m | 185 m | 100 m | 500 m | 100 m | 100 m |
| Nodos por segmento | 100 | 30 | 2 (un extremo es el hub y el otro el computador) | | | |

Los adaptadores pueden ser compatibles con varios de los estándares anteriores dando lugar a numerosas combinaciones. Sin embargo, lo habitual es encontrar en el mercado tarjetas de red de tan sólo estos dos tipos:

- *Tarjetas de red combo*. Tienen 2 conectores, uno para cable coaxial y otro para RJ45. Su velocidad máxima es de 10 Mbps por lo que soportan 10Base2 y 10BaseT. La tarjeta de red RTL8029 del fabricante Realtek pertenece a este tipo. Este grupo de tarjetas de red tienden a desaparecer (al igual que el cable coaxial).
- *Tarjetas de red 10/100*. Tienen sólo conector para RJ45. Se adaptan a la velocidad de la red (10 Mbps o 100 Mbps). Son compatibles con 10BaseT y 100BaseT. Como ejemplos de este tipo se encuentran las tarjetas Realtek RTL8139 y 3COM 3C905.

## *Preguntas propuestas*

1.- ¿Cuál es la función principal del nivel de enlace?

2.- ¿Qué problemas se analizan en el nivel de enlace?

3.- ¿Qué es una MAC?

4.- ¿los routers tienen dirección física?

5.- ¿Qué es la topología de red?

## *Respuestas a las preguntas propuestas*

1.-

- El tema principal es los algoritmos para la comunicación confiable y eficiente entre dos máquinas adyacentes.

2.-

- Los problemas de: los errores en los circuitos de comunicación, sus velocidades finitas de transmisión, y el tiempo de propagación.

3.-

- Dirección física

4.-

- Si

5.-

- La topología de red se define como la cadena de comunicación usada por los nodos que conforman una red para comunicarse.

Capítulo 6

# *CAPA DE RED*

## 6.1. La capa de red

El concepto de red está relacionado con las direcciones IP que se configuren en cada computador, no con el cableado. Es decir, si tenemos varias redes dentro del mismo cableado solamente los computadores que permanezcan a una misma red podrán comunicarse entre sí. Para que los computadores de una red puedan comunicarse con los de otra red es necesario que existan routers que interconecten las redes. Un router o encaminador no es más que un computador con varias direcciones IP, una para cada red, que permita el tráfico de paquetes entre sus redes.

La familia de protocolos TCP/IP fue diseñada para permitir la interconexión entre distintas redes. El mejor ejemplo de interconexión de redes es Internet: se trata de un conjunto de redes unidas mediante encaminadores o routers.

En una red TCP/IP es posible tener, por ejemplo, servidores web y servidores de correo para uso interno.

### Ejemplo de interconexión de 3 redes

Cada host (computador) tiene una dirección física que viene determinada por su adaptador de red. Estas direcciones se corresponden con la capa de acceso al medio y se utilizan para comunicar dos computadores que pertenecen a la misma red. Para identificar globalmente un computador dentro de un conjunto de redes TCP/IP se utilizan las direcciones IP (capa de red). Observando una dirección IP sabremos si pertenece a nuestra propia red o a una distinta (todas las direcciones IP de la misma red comienzan con los mismos números).

**Tabla 11**

| Host | Dirección física | Dirección IP | Red |
|---|---|---|---|
| A | 00-60-52-0B-B7-7D | 192.168.0.10 | Red 1 |
| R1 | 00-E0-4C-AB-9A-FF | 192.168.0.1 | |
| | A3-BB-05-17-29-D0 | 10.10.0.1 | Red 2 |
| B | 00-E0-4C-33-79-AF | 10.10.0.7 | |
| R2 | B2-42-52-12-37-BE | 10.10.0.2 | |
| | 00-E0-89-AB-12-92 | 200.3.107.1 | Red 3 |
| C | A3-BB-08-10-DA-DB | 200.3.107.73 | |
| D | B2-AB-31-07-12-93 | 200.3.107.200 | |

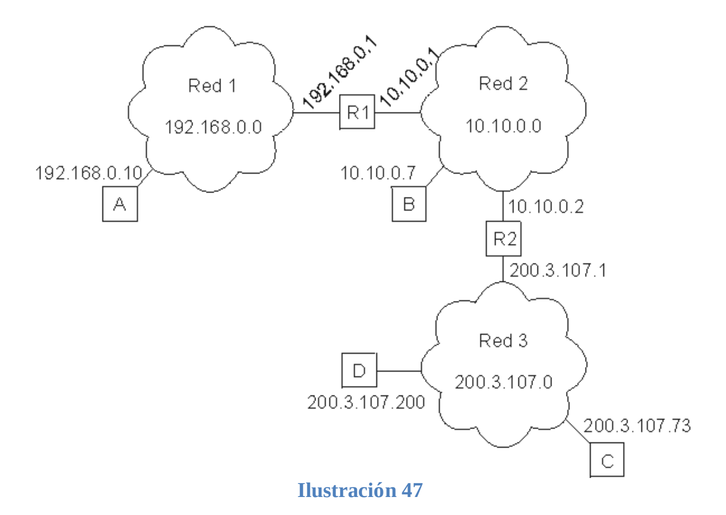



**Ilustración 47**

La capa de red se encarga de fragmentar cada mensaje en paquetes de datos llamados datagramas IP y de enviarlos de forma independiente a través de la red de redes. Cada datagrama IP incluye un campo con la dirección IP de destino. Esta información se utiliza para enrutar los datagramas a través de las redes necesarias que los hagan llegar hasta su destino.

Nota: Cada vez que visitamos una página web o recibimos un correo electrónico es habitual atravesar un número de redes comprendido

entre 10 y 20, dependiendo de la distancia de los hosts. El tiempo que tarda un datagrama en atravesar 20 redes (20 routers) suele ser inferior a 600 milisegundos.

En el ejemplo anterior, supongamos que el computador 200.3.107.200 (D) envía un mensaje al computador con 200.3.107.73 (C). Como ambas direcciones comienzan con los mismos números, D sabrá que ese computador se encuentra dentro de su propia red y el mensaje se entregará de forma directa. Sin embargo, si el computador 200.3.107.200 (D) tuviese que comunicarse con 10.10.0.7 (B), D advertiría que el computador destino no pertenece a su propia red y enviaría el mensaje al router R2 (es el computador que le da salida a otras redes). El router entregaría el mensaje de forma directa porque B se encuentra dentro de una de sus redes (la Red 2).

## *Protocolos de la capa de red*

Los protocolos que vamos a describir a continuación no se preocupan por el medio de transmisión: dan por hecho que existe un protocolo de la capa de acceso al medio que se encarga del envío y recepción de los paquetes a través del medio de transmisión.

### *IPX*

Protocolo IPX (*Internetwork Packet Exchange,* intercambio de paquetes entre redes) fue desarrollada por Novell a principios de los años 80. Gozó de gran popularidad durante unos 15 años si bien actualmente ha caído en desuso. Estos protocolos fueron creados como parte del sistema operativo de red Novell NetWare. En un principio fueron protocolos propietarios aunque más adelante se comenzaron a incorporar a otros sistemas operativos: Windows los incluye con los nombres de *Protocolo compatible con IPX/SPX* o *Transporte compatible NWLink IPX/SPX* según las versiones.

IPX es *enrutable*: hace posible la comunicación entre computadores pertenecientes a redes distintas interconectadas por encaminadores (*routers*). El protocolo IPX pertenece a la capa de red y se encarga del envío de los paquetes (fragmentos de mensajes) a través de las redes necesarias para llegar a su destino.

La estructura de protocolos IPX/SPX se corresponde en gran medida con TCP/IP. Su configuración es más sencilla que en TCP/IP aunque admite menos control sobre el direccionamiento de la red. El

identificador de cada puesto en la red es un número de 6 bytes, que coincide con la dirección física de su adaptador, seguido de un número de 6 bytes, que representa la dirección de la red. Por ejemplo: 44.45.EA.54.00.00:4C.34.A8.59 (nodo: red).

***AppleTalk***

Es el protocolo propietario de Apple utilizado para interconectar computadores Macintosh. Es un protocolo enrutable. El identificador de cada puesto es un número de 1 byte y el de cada red, un número de 2 bytes. Por ejemplo, "50.8" representa el computador 8 de la red 50. Si el número de puestos en una red es superior a 253 hosts, se utilizan varios números de redes contiguos en lugar de sólo uno. Por ejemplo, la red "100-101" dará cabida a 506 hosts. Un host conectado a la red "100-101" tendrá una dirección de la forma "100.*x*". En la terminología de Apple, una red se conoce como una *zona*.

***NetBEUI***

NetBEUI (*NetBIOS Extended User Interface*, interfaz de usuario extendida para NetBIOS) es un protocolo muy sencillo que se utiliza en redes pequeñas de menos de 10 computadores que no requieran salida a Internet. Su funcionamiento se basa en el envío de difusiones a todos los computadores de su red. Sus difusiones no atraviesan los encaminadores a no ser que estén configurados para dejar pasar este tráfico: es un protocolo no enrutable.

La ventaja de este protocolo es su sencillez de configuración: basta con instalar el protocolo y asignar un nombre a cada computador para que comience a funcionar. Su mayor desventaja es su ineficiencia en redes grandes (se envían excesivas difusiones).

Actualmente es un protocolo exclusivo de las redes Microsoft. Fue diseñado para ofrecer una interfaz sencilla para NetBIOS (este protocolo trabaja en la capa de aplicación).

***IP***

IP (*Internet Protocol*, protocolo de Internet) es el estándar en las redes. Fue diseñado por el Departamento de Defensa de los Estados Unidos a finales de los años 70 para utilizarse en una red resistente a bombas: aunque se destruyese alguna línea de comunicación o encaminador, la comunicación podría seguir funcionando por rutas alternativas. Lo sorprendente de TCP/IP es que no fue pensado para

resistir el espionaje: los protocolos originales transmiten las contraseñas y datos sin codificación alguna.

IP es el protocolo de Internet (en realidad, es una familia de protocolos). En la actualidad es la elección recomendada para casi todas las redes, especialmente si la red tiene salida a Internet.

El protocolo IP, perteneciente a la capa de red. El identificador de cada puesto es la *dirección IP*. Una dirección IP es un número de 4 bytes. Por ejemplo: 194.142.78.95. Este número lleva codificado la dirección de red y la dirección de host

Las direcciones IP se clasifican en:

- *Direcciones públicas*. Son visibles desde todo Internet. Se contratan tantas como necesitemos. Son las que se asignan a los servidores de Internet que sirven información 24 horas al día (por ejemplo, un servidor web).
- *Direcciones privadas*. Son visibles sólo desde una red interna pero no desde Internet. Se utilizan para identificar los puestos de trabajo de las empresas. Se pueden utilizar tantas como se necesiten; no es necesario contratarlas.

### *Familia de protocolos TCP/IP*

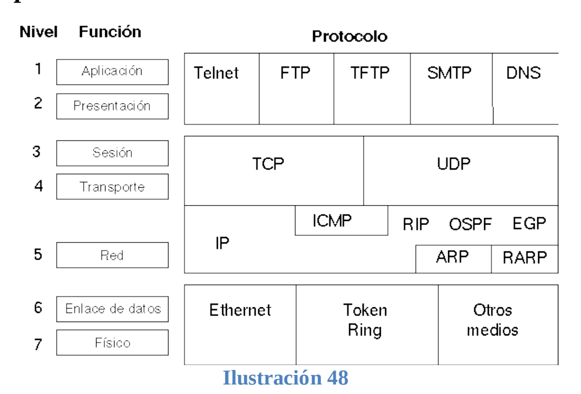



**Ilustración 48**

## *Preguntas propuestas*

1.- ¿Cuál es la función del nivel de red?

2.- ¿Qué fin cumple el nivel de red?

3.- ¿Qué decisión realiza el nivel de red?

***Respuestas a las preguntas propuestas***

1.-

- Ruteo de los paquetes de la fuente al destino final a través de ruteadores intermedios. Tiene que saber la topología de la subred, evitar la congestión, y manejar los casos cuando la fuente y el destino están en redes distintas.

2.-

- El nivel de red normalmente es la interfaz entre el portador y el cliente. Sus servicios son los servicios de la subred. Fines:
    - Los servicios debieran ser independientes de la tecnología de la subred.
    - Se debiera resguardar el nivel de transporte de las características de las subredes.
    - Las direcciones de red disponibles al nivel de transporte debieran usar un sistema uniforme.

3.-

- La gran decisión en el nivel de red es si el servicio debiera ser orientado a la conexión o sin conexión.
    - Sin conexión (Internet). La subred no es confiable; porta bits y no más. Los hosts tienen que manejar el control de errores. El nivel de red ni garantiza el orden de paquetes ni controla su flujo. Los paquetes tienen que llevar sus direcciones completas de destino.
    - Orientado a la conexión (sistema telefónico). Los pares en el nivel de red establecen conexiones con características tal como la calidad, el costo, y el ancho de banda. Se entregan los paquetes en orden y sin errores, la comunicación es dúplex, y el control de flujo es automático.

Capítulo 7

# *CAPA DE TRANSPORTE*

## 7.1. La capa de transporte

### ***Protocolos de la capa de transporte***

#### ***SPX***

El protocolo SPX (*Sequential Packet Exchange*, intercambio de paquetes secuenciales).

SPX es *enrutable*: hace posible la comunicación entre computadores pertenecientes a redes distintas interconectadas por encaminadores (*routers*). El protocolo SPX pertenece a la capa de transporte: gestiona el envío de mensajes completos entre los dos extremos de la comunicación.

#### ***TCP***

TCP (*Transport Control Protocol*, protocolo de control de transporte)

TCP es el protocolo de Internet

El protocolo TCP, perteneciente a la capa de transporte.

Capítulo 8

# *REDES INALAMBRICAS*

## 8.1. Introducción

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. La conexión de computadoras mediante Ondas de Radio o Luz Infrarroja, actualmente está siendo ampliamente investigada. Las Redes Inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos.

Las redes inalámbricas se han desarrollado vertiginosamente en los últimos años

Las tecnologías más usadas actualmente son la IEEE802.11b y g

La tecnología emergente IEEE802.11n es muy prometedora y los costos bajan rápido

Pronto el acceso inalámbrico se podrá hacer en cualquier parte: trabajo, hogar, café, automóvil, tren, etc. y las aplicaciones son ilimitadas.

La seguridad es de suma importancia

## 8.2. Redes de acceso inalámbrico

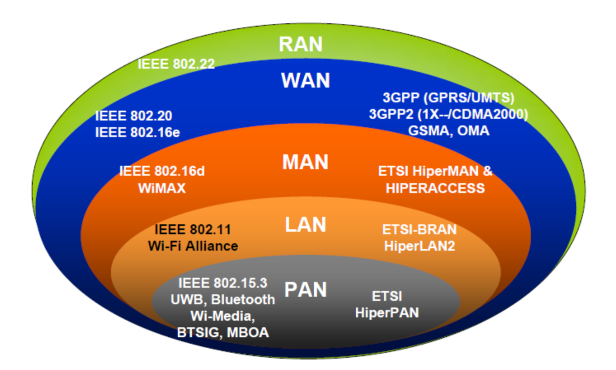
En estas redes los clientes se conectan a la red usando señales de radio en reemplazo del cobre, en parte o en toda la conexión entre el cliente y la central de conmutación.

Técnica de acceso muy utilizada en regiones donde las redes están aún en desarrollo. También en países de reciente apertura en competencia resulta ideal para un rápido despliegue de red

## 8.3. Clasificación de las redes inalámbricas

- WLL (Wireless Local Loop)
- Broadband Wireless
  - WiFi
  - Wimax
  - LMDS
  - MMDS
  - FOS
- Sistemas celulares

## 8.4. Estándares inalámbricos




## 8.5. Tecnologías inalámbricas

| Technology | Frequency Band | Applications |
|---|---|---|
| Cellular | 824-894M | Cellular |
| PCS | 1.850-1.990G | Cellular |
| MMDS | 2.5-2.7G | MAN/WAN |
| ISM (802.11b) | 2.4-2.48G | LAN |
| U-NNI (802.11a) | 5.725-5.875G | LAN |
| **802.16-2004** | **2-11 and 10-66 GHz** | **MAN/WAN** |
| LMDS | 27.5-31.3GHz | MAN/WAN |

## 8.6. WiFi

Es un conjunto de estándares para redes inalámbricas basado en las especificaciones IEEE 802.11.

Wi-Fi se creó para ser utilizada en redes locales inalámbricas, pero es frecuente que en la actualidad también se utilice para acceder a Internet.

Wi-Fi es una marca de la Wi-Fi Alliance (anteriormente la Wireless Ethernet Compatibility Alliance), la organización comercial que prueba y certifica que los equipos cumplen los estándares IEEE 802.11x.

Los estándares IEEE 802.11b e IEEE 802.11g disfrutan de una aceptación internacional debido a que la banda de 2.4 GHz está disponible casi universalmente, con una velocidad de hasta 11 Mbps y 54 Mbps. Existe también el estándar IEEE 802.11n que está en desarrollo y trabaja a 2.4 GHz a una velocidad de 108 Mbps.

En los Estados Unidos y Japón, se maneja también el estándar IEEE 802.11a, conocido como WIFI 5, que opera en la banda de 5 GHz y que disfruta de una operatividad con canales relativamente limpios.

APLICACIONES

- Distribución multimedia
- Transporte público
- Instrumentación
- Teletrabajo

## 8.7. WiMaX

Del inglés Worldwide Interoperability for Microwave Access, Interoperabilidad Mundial para Acceso por Microondas) es un estándar de transmisión inalámbrica de datos (802.16d) diseñado para ser utilizado en el área metropolitana o MAN.

Un sistema de WiMax tiene dos partes:

- Por un lado están las torres WiMax, que dan cobertura de hasta 8.000 km cuadrados según el tipo de señal transmitida
- Por otro están los receptores, es decir, las tarjetas que conectamos a nuestro PC, portátil, PDA y demás para tener acceso.

Esta tecnología de acceso transforma las señales de voz y datos en ondas de radio dentro de la citada banda de frecuencias. Está basada en OFDM, y con 256 subportadoras puede cubrir un área de 48 kilómetros, usualmente sin la necesidad de contar con línea de vista entre emisor y receptor, y sin la necesidad de pagar consumo

telefónico; con capacidad para transmitir datos a una tasa de hasta 75 Mbps, con una eficiencia espectral de 5.0 bps/Hz y con una escalabilidad de canales de 1,5 MHz a 20 MHz

WiMAX se sitúa en un rango intermedio de cobertura entre las demás tecnologías de acceso de corto alcance y ofrece velocidades de banda ancha para un área metropolitana.

El IEEE aprobó el estándar del WiMAX MÓVIL, el 802.16e, que permite utilizar este sistema de comunicaciones inalámbricas con terminales en movimiento.

En Corea se ha materializado las ventajas de un WiMAX móvil trabajando en 2,3Ghz y se le ha acuñado el nombre de WiBRO (Wireless Broadband )

APLICACIONES

- Teletrabajo
- Telemedicina
- Gestión de servicios públicos
- Comercio electrónico

## 8.8. Estándares

- 802.11
- 802.11a
- 802.11b
- 802.11d
- 802.11e
- 802.11f
- 802.11g
- 802.11h
- 802.11i
- 802.11n

802.11 Estándar WLAN original. Soporta de 1 a 2 Mbps

802.11a Estándar WLAN de alta velocidad en la banda de los 5 GHz. Soporta hasta 54 Mbps. Utiliza el método de modulación OFMD (Múltiplexación por división de frecuencias octogonales), en transmisiones exteriores hay un alcance de 30mts a 300mts y en interiores de 12mts a 90mts, entre mayor distancia menos velocidad.

802.11b Estándar WLAN para la banda de 2.4 GHz. Soporta 11 Mbps. Utiliza el método de modulación DSSS (Modulación de frecuencias directas del espectro extendido)

802.11d Itinerancia internacional, configura dispositivos automáticamente para que cumplan con los regulaciones locales

802.11e Está dirigido a los requisitos de calidad de servicio para todas las interfaces IEEE WLAN de radio.

802.11f Define la comunicación entre puntos de acceso para facilitar redes WLAN de diferentes proveedores.

802.11g Establece una técnica de modulación adicional para la banda de los 2.4 GHz. Dirigido a proporcionar velocidades de hasta 54 Mbps. El método de modulación que utiliza es el OFMD (Multiplexacion por división de frecuencias octogonales) y también DSSS (Modulación de frecuencias directas del espectro extendido)

802.11i Está dirigido a abatir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1X, TKIP (Protocolo de Llaves Integras – Seguras– Temporales), y AES (Estándar de Cifrado Avanzado).

802.11n Proporciona mejoras de mayor capacidad de proceso, se pretende que la proporción de velocidades es de 500Mbs

802.11h Define la administración del espectro de la banda de los 5 GHz para su uso en Europa y en Asia Pacífico.

| Estándares Wireless | | | |
|---|---|---|---|
| Estándar | 802.11b | 802.11a | 802.11g |
| Aprobado IEEE | Julio 1999 | Julio 1999 | Junio 2003 |
| Popularidad | Adoptado masivamente | Nueva tecnología, crecimiento bajo | Nueva tecnología, con un rápido crecimiento |
| Velocidad | Hasta 11 Mbps. | Hasta 54 Mbps. | |
| Coste | Barato | Relativamente caro | Relativamente barato |
| Frecuencia | 2.4 - 2.497 Ghz | 5.15 - 5.35 Ghz<br>5.425 - 5.675 Ghz<br>5.725 - 5.875 Ghz | 2.4 - 2.497 Ghz |
| Cobertura | Buena cobertura, unos 300 - 400 metros, con buena conectividad con determinados obstáculos | Cobertura baja, unos 150 metros, con mala conectividad con obstáculos | Buena cobertura, unos 300 - 400 metros, con buena conectividad con determinados obstáculos |

**Estándar WiMAX:**

| | 802.16 | 802.16a | 802.16e |
|---|---|---|---|
| **Espectro** | 10 - 66 GHz | < 11 GHz | < 6 GHz |
| **Funcionamiento** | Solo con visión directa | Sin visión directa (NLOS) | Sin visión directa (NLOS) |
| **Tasa de bit** | 32 - 134 Mbit/s con canales de 28 MHz | Hasta 75 Mbit/s con canales de 20 MHz | Hasta 15 Mbit/s con canales de 5 MHz |
| **Modulación** | QPSK, 16QAM y 64 QAM | OFDM con 256 subportadoras QPSK, 16QAM, 64QAM | Igual que 802.16a |
| **Movilidad** | Sistema fijo | Sistema fijo | Movilidad pedestre |
| **Anchos de banda** | 20, 25 y 28 MHz | Seleccionables entre 1,25 y 20 MHz | Igual que 802.16a con los canales de subida para ahorrar potencia |
| **Radio de celda típico** | 2 - 5 km aprox. | 5 - 10 km aprox. (alcance máximo de unos 50 km) | 2 - 5 km aprox. |

## 8.9. Formas de conexión

- Puntos de acceso
- Repetidores
- Enrutadores
- Puentes
- Adaptadores

PUNTOS DE ACCESO

Es la unidad de conexión central entre la red cableada y los dispositivos WLAN. Actúan como un hub que facilita conectar uno o varios nodos de forma inalámbrica a una red cableada. Como funciones adicionales normalmente consideran el control de seguridad de la red.

Tipos Puntos de Acceso

- Puntos de Acceso B y G: Transmite paquetes entre 11 Mbit/s y 20Mbit/s en la banda de 2.4Ghz en el estándar B y paquetes hasta 54Mbit/s en la banda de 2.4Ghz en el estándar G, utilizando los sistemas WEP y WAP.
- Puntos de acceso A+G: Transmite paquetes a 6Mbit/s en una banda de 5.0Ghz en el estándar A y no ofrece seguridad, y paquetes hasta 54Mbit/s en la banda de 2.4Ghz en el estándar G, utilizando los sistemas WEP y WAP.

REPETIDORES

Dispositivo hardware encargado de amplificar o regenerar la señal entre dos segmentos de una red homogénea. Operan a nivel físico del modelo de OSI. También conocido como expansor de rango o antena de expansión.

ENRUTADORES

Interfaz entre la red local LAN e Internet, coordina el envío y recepción de paquetes de datos entre el ordenador local e Internet.

PUENTES

Dispositivo que tienen usos definidos. Interconectan segmentos de la red a través de medios físicos diferentes. En algunas ocasiones pueden manejar múltiples redes de datos.

ADAPTADORES

Dispositivos con los cuales se logra conectar un nodo a una red inalámbrica.

## 8.10. Seguridad Inalámbrica

- Filtrado MAC
- Seguridad básica WEP y avanzada WPA
- 802.1x

- Túneles VPN

Filtrado de direcciones MAC

Este método consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica. Dicha tabla contiene las direcciones MAC (Media Access Control) de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo. Este método tiene como ventaja su sencillez, por lo cual se puede usar para redes caseras o pequeñas. Sin embargo, posee muchas desventajas que lo hacen impráctico para uso en redes medianas o grandes:

Desventajas del filtrado MAC

- No escala bien, porque cada vez que se desee autorizar o dar de baja un equipo, es necesario editar las tablas de direcciones de todos los puntos de acceso.
- Después de cierto número de equipos o de puntos de acceso, la situación se torna inmanejable.
- El formato de una dirección MAC no es amigable (normalmente se escriben como 6 bytes en hexadecimal), lo que puede llevar a cometer errores en la manipulación de las listas.
- Las direcciones MAC viajan sin cifrar por el aire. Un atacante podría capturar direcciones MAC de tarjetas matriculadas en la red empleando un sniffer, y luego asignarle una de estas direcciones capturadas a la tarjeta de su computador, empleando programas tales como AirJack6 o WellenReiter, entre otros. De este modo, el atacante puede hacerse pasar por un cliente válido.
- En caso de robo de un equipo inalámbrico, el ladrón dispondrá de un dispositivo que la red reconoce como válido. En caso de que el elemento robado sea un punto de acceso el problema es más serio, porque el punto de acceso contiene toda la tabla de direcciones válidas en su memoria de configuración. Debe notarse además, que este método no garantiza la confidencialidad de la información transmitida, ya que no prevé ningún mecanismo de cifrado.

Wired Equivalent Privacy (WEP)

El algoritmo WEP10 forma parte de la especificación 802.11, y se diseñó con el fin de proteger los datos que se transmiten en una conexión inalámbrica mediante cifrados. WEP opera a nivel 2 del modelo OSI y es soportado por la gran mayoría de fabricantes de soluciones inalámbricas.

El algoritmo WEP cifra de la siguiente manera:

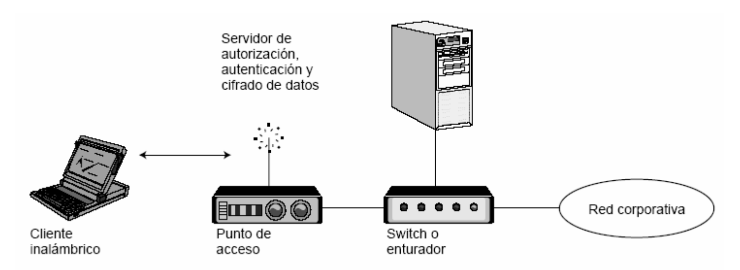
Se escoge una clave secreta compartida entre emisor y receptor. Esta clave puede poseer 40 ó 128 bits.

Desventajas de WEP

WEP no ofrece servicio de autenticación. El cliente no puede autenticar a la red, ni al contrario; basta con que el equipo móvil y el punto de acceso compartan la clave WEP para que la comunicación pueda llevarse a cabo. Existen en este momento diversas herramientas gratuitas para romper la clave secreta de enlaces protegidos con WEP. El primer programa que hizo esto posible fue WEPCrack, que consiste en una serie de scripts escritos en lenguaje Perl diseñados para analizar un archivo de captura de paquetes de un sniffer. La herramienta AirSnort hace lo mismo, pero integra las funciones de sniffer y rompedor de claves, y por lo tanto es más fácil de usar. Airsnort captura paquetes pasivamente, y rompe la clave WEP cuando ha capturado suficientes datos.

Túneles VPN

- Una red privada virtual (Virtual Private Network, VPN) emplea tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público. La parte de la red que maneja el acceso inalámbrico debe estar aislada del resto de la red, mediante el uso de una lista de acceso adecuada en un enrutador, o agrupando todos los puertos de acceso inalámbrico en una VLAN si se emplea switching.
- La VLAN solamente debe permitir el acceso del cliente inalámbrico a los servidores de autorización y autenticación de la VPN.
- Los servidores de VPN se encargan de autenticar y autorizar a los clientes inalámbricos, y de cifrar todo el tráfico desde y hacia dichos clientes. Dado que los datos se cifran en un nivel superior del modelo OSI, no es necesario emplear WEP en este esquema.




Estructura de una VPN para acceso inalámbrico seguro

802.1x

- 802.1x es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red.
- El protocolo 802.1x involucra tres participantes:
  - El suplicante
  - El servidor de autorización/autenticación
  - El autenticador

***El suplicante***

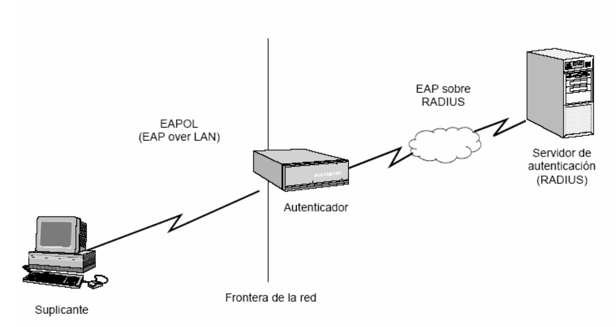
Equipo del cliente, que desea conectarse con la red

***El servidor de autorización/autenticación***

Contiene toda la información necesaria para saber cuáles equipos y/o usuarios están autorizados para acceder a la red.

***El autenticador***

Es el equipo de red que recibe la conexión del suplicante.




**Arquitectura de un sistema de autentificación 802.1x**

## WPA (WI-FI Protected Access)

WPA propone un nuevo protocolo para cifrado, conocido como TKIP (Temporary Key Integrity Protocol). Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. Igualmente se mejoraron los algoritmos de cifrado de trama, con respecto a WEP.

La norma WPA data de abril de 2003, y es de obligatorio cumplimiento para todos los miembros de la Wi-Fi Alliance a partir de finales de 2003. Según la Wi-Fi Alliance, todo equipo de red inalámbrica que posea el sello “Wi- Fi Certified” podrá ser actualizado por software para que cumpla con la especificación WPA.



## 8.11. Fabricantes de equipo inalámbrico

Entre los principales fabricantes de equipos para wireless podemos citar:

- MSI
- Linksys
- D-Link
- Zoom (propiamente el modelo X6 para ADSL)
- CISCO SYSTEMS



## *Bibliografía*

### *Textos*


- ***ALCÓCER, Carlos***. *Redes de Computadoras. Infolink. Segunda Edición. 2000. Lima*
- ***TANENBAUM, Andrew S***. *Redes de computadoras. Pearson. Cuarta edición. 1998*
- ***GOMEZ V., Alvaro, VELOSO E., Manuel***. *Redes de computadoras e internet. Alfaomega Ra-Ma. Primera edición. 2005*
- ***GARCIA, P. DIAZ, J. LOPEZ, J***. *Transmisión de Datos y Redes de Computadores. Pearson. Prentice Hall. 2003*
- ***STALLINGS, William***. Comunicaciones y redes de computadores. *Prentice Hall*. Séptima *edición. 2000*
- ***JIMÉNEZ ROCHABRUM***, ***Gerardo.*** "Redes y Cableado Estructurado". Empresa Editora RITISA. 1ra.Edicion. Pág. 92. Perú. 2005.
- **LEÓN-GARCÍA**, **Alberto**, **WIDJAJA**, **Indra**. "Redes de Comunicación". Editorial Mc Graw Hill. Pág. 43. España. 2002.


### *Direcciones Electrónicas*


- Cisco redes sin fronteras: http://www.cisco.com/web/LA/soluciones/network_index.html#~acc~business_case
- Networking HP-3COM: http://h17007.www1.hp.com/us/en/
- Network adapter D-Link: http://www.dlinkla.com/home/productos/familia.jsp?id_fam=3
- Simulador AP TP-Link: http://www.tp-link.com/simulator/TL-WA501G/userRpm/index.htm
- Fast Ethernet ENCORE: http://www.encore-usa.com/co/cat/Wired-Networking/Fast-Ethernet-100Mbps
- Switches con controladores de acceso a redes EDIMAX: http://edimax.es/es/produce_list.php?pl1_id=14&pl2_id=44

# *Apéndice*

## *Comandos de Redes*

- ***arp*** – Muestra y permite modificar las tablas del protocolo ARP, encargado de convertir las direcciones IP de cada ordenador en direcciones MAC (dirección física única de cada tarjeta de red), ejemplo, c:\arp –a

```
C:\Windows\system32\cmd.exe

C:\Users\luis>arp -a

Interfaz: 192.168.0.252 --- 0xd
  Dirección de Internet          Dirección física      Tipo
  192.168.0.255         ff-ff-ff-ff-ff-ff     estático
  192.168.1.1           00-02-cf-bf-4b-78     dinámico
  224.0.0.252           01-00-5e-00-00-fc     estático
  224.0.0.253           01-00-5e-00-00-fd     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático

C:\Users\luis>
```

- ***ftp*** – Cliente FTP en modo consola de comandos
- ***getmac*** – Muestra las direcciones MAC de los adaptadores de red que tengamos instalados en el sistema, ejemplo, c:\getmac

```
C:\Windows\system32\cmd.exe
C:\Users\luis>getmac

Dirección física    Nombre de transporte
=================== ==========================================================
N/A                 Hardware ausente
00-1B-11-B7-B1-B2   \Device\Tcpip_{793578B4-79CF-4858-894A-1A9960B12F0B}
06-1B-11-B7-B1-B2   Medios desconectados

C:\Users\luis>
```

- ***ipconfig*** – Muestra y permite renovar la configuración de todos los interfaces de red, ejemplo, c:\ipconfig

```
C:\Windows\system32\cmd.exe

C:\Users\luis>ipconfig

Configuración IP de Windows


Adaptador de LAN inalámbrica Conexión de red inalámbrica 2:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Conexión de red inalámbrica:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::885b:87f7:4323:5bf4%13
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.0.252
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.1.252
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.100.252
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.1.1

Adaptador de túnel isatap.{793578B4-79CF-4858-894A-1A9960B12F0B}:

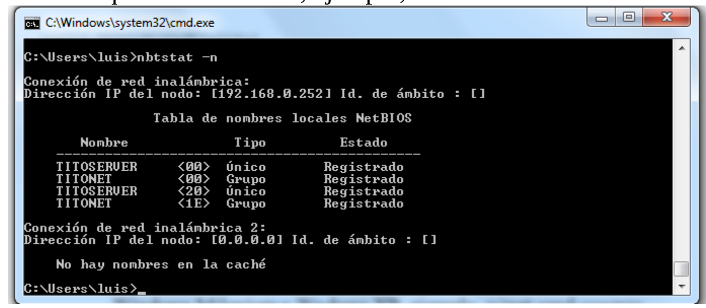
   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de túnel Teredo Tunneling Pseudo-Interface:

   Sufijo DNS específico para la conexión. . :
   Dirección IPv6 . . . . . . . . . . : 2001:0:4137:9e76:8a0:a1c5:360f:ea6f
   Vínculo: dirección IPv6 local. . . : fe80::8a0:a1c5:360f:ea6f%18
   Puerta de enlace predeterminada . . . . . : ::

C:\Users\luis>
```

- ***msg*** – sirve para enviar mensaje en una red LAN, para Windows Vista y Wndows 7, ejemplo, c:\msg *usuario* “mensaje”
- ***nbtstat*** – Muestra las estadísticas y las conexiones actuales del protocolo NetBIOS sobre TCP/IP, los recursos compartidos y los recursos que son accesibles, ejemplo, c:\nbtstat -n



```
C:\Windows\system32\cmd.exe

C:\Users\luis>nbtstat -n

Conexión de red inalámbrica:
Dirección IP del nodo: [192.168.0.252] Id. de ámbito : []

                Tabla de nombres locales NetBIOS

       Nombre               Tipo            Estado
    ---------------------------------------------
    TITOSERVER      <00>  Único          Registrado
    TITONET         <00>  Grupo          Registrado
    TITOSERVER      <20>  Único          Registrado
    TITONET         <1E>  Grupo          Registrado

Conexión de red inalámbrica 2:
Dirección IP del nodo: [0.0.0.0] Id. de ámbito : []

    No hay nombres en la caché

C:\Users\luis>_
```

- ***net*** – Permite administrar usuarios, carpetas compartidas, servicios, etc. Para Windows Vista y Wndows 7. Para un listado completo de todas las opciones, escribir net sin ningún argumento. Para obtener ayuda sobre alguna opción en concreto, escribier net help opción
- ***net send*** – sirve para enviar mensaje en una red LAN, para Windows Milenium y Wndows XP, ejemplo, c:\net send *usuario* “mensaje”
- ***netsh*** – Programa en modo consola permite ver, modificar y diagnosticar la configuración de la red

- ***netstat*** – Información sobre las conexiones de red de nuestro equipo, ejemplo, c:\netstat

```
C:\Windows\system32\cmd.exe

C:\Users\luis>netstat

Conexiones activas

  Proto  Dirección local          Dirección remota         Estado
  TCP    192.168.1.252:50577      195-114-19-85:http       CLOSE_WAIT
  TCP    192.168.1.252:52245      client-200:http          TIME_WAIT
  TCP    192.168.1.252:52310      us:http                  TIME_WAIT
  TCP    192.168.1.252:52331      us:http                  TIME_WAIT
  TCP    192.168.1.252:52336      client-200:http          ESTABLISHED
  TCP    192.168.1.252:52341      ec2-174-129-1-163:http   TIME_WAIT

C:\Users\luis>
```

- ***nslookup*** – Aplicación de red orientada a obtener información en los servidores DNS sobre un host en concreto, ejemplo, c:\nslookup

```
C:\Windows\system32\cmd.exe - nslookup

C:\Users\luis>nslookup
Servidor predeterminado:  cachewas.tdp.net.pe
Address:  200.48.225.130

>
```

- ***pathping*** – Muestra la ruta que sigue cada paquete para llegar a una IP determinada, el tiempo de respuesta de cada uno de los nodos por los que pasa y las estadísticas de cada uno de ellos, ejemplo, c:\pathping –g 190.40.3.3

```
C:\Windows\system32\cmd.exe

C:\Users\luis>pathping -g 190.40.3.3

Traza a 190.40.3.3 sobre caminos de 30 saltos como máximo.

  0  titoserver [192.168.1.252]
  1  192.168.1.1
  2     *           *           *
Procesamiento de estadísticas durante 25 segundos...
              Origen hasta aquí   Este Nodo/Vínculo
Salto  RTT    Perdido/Enviado = Pct  Perdido/Enviado = Pct  Dirección
  0                                           titoserver [192.168.1.252]
                                 18/ 100 = 18%   |
  1    7ms    18/ 100 = 18%       0/ 100 =  0%  192.168.1.1

Traza completa.

C:\Users\luis>_
```

- ***ping*** – Comando para comprobar si una máquina está en red o no, ejemplo, c:\ping 192.168.1.252

```
C:\Windows\system32\cmd.exe

C:\Users\luis>ping 192.168.1.252

Haciendo ping a 192.168.1.252 con 32 bytes de datos:
Respuesta desde 192.168.1.252: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.252: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.252: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.252: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.1.252:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\luis>_
```

- ***rasdial*** – Permite establecer o finalizar una conexión telefónica
- **route** – Permite ver o modificar las tablas de enrutamiento de red, ejemplo, c:\route print

```
C:\Windows\system32\cmd.exe
C:\Users\luis>route print
===========================================================================
ILista de interfaces
 17...06 1b 11 b7 b1 b2 ......Microsoft Virtual WiFi Miniport Adapter
 13...00 1b 11 b7 b1 b2 ......Adaptador PCI inalámbrico D-Link AirPlus DWL-G520
(rev.B)
  1...........................Software Loopback Interface 1
 19...00 00 00 00 00 00 00 e0 Adaptador ISATAP de Microsoft
 18...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
===========================================================================

IPv4 Tabla de enrutamiento
===========================================================================
Rutas activas:
Destino de red        Máscara de red   Puerta de enlace   Interfaz  Métrica
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.0.252    281
        127.0.0.0        255.0.0.0      En vínculo         127.0.0.1    306
        127.0.0.1  255.255.255.255      En vínculo         127.0.0.1    306
  127.255.255.255  255.255.255.255      En vínculo         127.0.0.1    306
      192.168.0.0    255.255.255.0      En vínculo     192.168.0.252    281
    192.168.0.252  255.255.255.255      En vínculo     192.168.0.252    281
    192.168.0.255  255.255.255.255      En vínculo     192.168.0.252    281
      192.168.1.0    255.255.255.0      En vínculo     192.168.0.252    281
    192.168.1.252  255.255.255.255      En vínculo     192.168.0.252    281
    192.168.1.255  255.255.255.255      En vínculo     192.168.0.252    281
    192.168.100.0    255.255.255.0      En vínculo     192.168.0.252    281
  192.168.100.252  255.255.255.255      En vínculo     192.168.0.252    281
  192.168.100.255  255.255.255.255      En vínculo     192.168.0.252    281
        224.0.0.0        240.0.0.0      En vínculo         127.0.0.1    306
        224.0.0.0        240.0.0.0      En vínculo     192.168.0.252    281
  255.255.255.255  255.255.255.255      En vínculo         127.0.0.1    306
  255.255.255.255  255.255.255.255      En vínculo     192.168.0.252    281
===========================================================================
Rutas persistentes:
  Dirección de red  Máscara de red  Dirección de puerta de enlace  Métrica
          0.0.0.0          0.0.0.0      192.168.1.1  Predeterminada
          0.0.0.0          0.0.0.0      192.168.1.1  Predeterminada
===========================================================================
```

- ***tracert*** – Informa sobre el camino que siguen los paquetes IP desde que sale de nuestra máquina hasta que llega a su destino, ejemplo, c:\tracert 190.40.3.3

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\luis>tracer 190.40.3.3
"tracer" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\luis>tracert 190.40.3.3

Traza a 190.40.3.3 sobre caminos de 30 saltos como máximo.

  1     6 ms     2 ms     9 ms  192.168.1.1
  2     *        *        *     Tiempo de espera agotado para esta solicitud.
  3     *        *        *     Tiempo de espera agotado para esta solicitud.
  4     *        *        *     Tiempo de espera agotado para esta solicitud.
  5    22 ms    25 ms    21 ms  10.115.0.24
  6    32 ms    35 ms    57 ms  190.40.3.1
  7    34 ms    37 ms    33 ms  190.40.3.3

Traza completa.

C:\Users\luis>_
```